II7MAD99@GMAIL.COM 26 Oct 2021

الاتصالات التطبيقات

شرح مفصل عن فحص تطبيقات Apple
وفك حمايتها مع ذكر الطلبات التابعة لها

فلاح العنزي

II7MAD99@GMAIL.COM 26 Oct 2021

رخصة الكتاب

هذا الكتاب يخضع لرخصه المشاع الإبداعي

لك الحق في نسخ الكتاب عند اتلافه كما تشاء، ولكن لا يسمح لك بيعه وتعديل عليه او ذكر محتوي الكتاب او نشره في تطبيقات التواصل

Telecom Applications © by FaLaH is licensed under CC BY-NC-ND 4.0

وفقاً للشروط عدم التزامك بها ستحاسب وجب القانون

لمن هذا الكتاب؟

اريد اجعل هذا الكتاب مفيدًا لفئات عديدة من القراء المبتدئين في مجال فحص التطبيقات من الصفر

II7MAD99@GMAIL.COM 26 Oct 2021

الكاتب

فلاح العنزي مبرمج وهكر أخلاقي

Flaaah777@gmail.com

سناب

Flaah999

اهداء

إلي أمي وأبي حفظهم الله

II7MAD99@GMAIL.COM 26 Oct 2021

المقدمة

هل سئلت نفسك يوم ما كيف تعمل التطبيقات؟

او كيف يكون ارسال المعلومات من هاتفك للتطبيق؟

في الكتاب سوف اعطيك كامل الإجابات

مع التطبيق على تطبيقات مشهوره

مثل snapchat / twitter :وغيرها..

II7MAD99@GMAIL.COM 26 Oct 2021

حماية التطبيقات

بعض التطبيقات المشهورة مثل سناب شات
تستخدم شهادة SSL والتي تمنع اغلب الأشخاص من الفحص
ويوجد تطبيقات لا تستخدم SSL ومن السهل فحصها بدون مشاكل

المعنى ماهي ضرورية للتطبيق ولكن نقدر نقول انها طبقة حماية
والشركة هي الي تقرر وليس المستخدمين

واغلب الشركات عند وضع SSL تعنى رسالة العب بعيد

ولكن يوجد طرق لأفتح الحماية بسهوله تامه
من أحد الأدوات الجلبريك وبرامج الكمبيوتر

II7MAD99@GMAIL.COM 26 Oct 2021

المتطلبات

- كمبيوتر
- ايفون
- جلبريك

نحتاج الكمبيوتر لأفحص تطبيقات الايفون

نحتاج ايفون لتحميل التطبيقات من أبل ستور

نحتاج جلبريك عشان نكسر حماية SSL للتطبيق - وليس لكل التطبيقات بعضها ما فيها

مثل تطبيق YOLO لا يوجد به شهادة SSL يعني لا نحتاج الجلبريك في الوقت نفسه والعكس مثل Snapcat نحتاج جلبريك لافك الحماية

II7MAD99@GMAIL.COM 26 Oct 2021

فوائد الجلبريك في الايفون

- التعديل على ملفات التطبيقات
- اضافه مميزات اضافيه للتطبيقات
- حماية جهازك من التتبع
- تنظيف جهازك من الملفات غير مرغوب بها
- نسخ الملفات الحساسة في التطبيقات
- تثبيت التطبيقات بدون شهادة ابل المطورين
- كسر حماية التطبيقات عند الفحص
- تعديل في نظام ابل مثل تركيب ثيم وغيرها

II7MAD99@GMAIL.COM 26 Oct 2021

تثبيت الأساسيات على الكمبيوتر

تحتاج برنامج Burp Suite Community Edition لكي تفحص تطبيقات الايفون بدونه لا تستطيع فحصها بشكل سلس

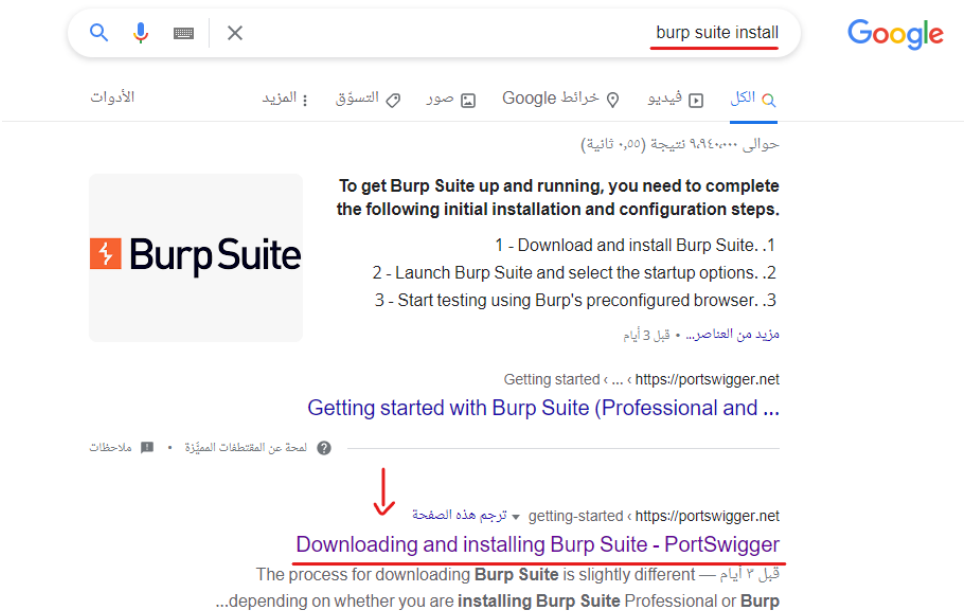
إذا ما تعرف تطبيق Burp Suite هو برنامج يستعرض لك الطلبات التطبيقات او مواقع الويب بعطيك مثال :

عند تسجيل الدخول في سناب شات يطلب منك اسم المستخدم وكلمة المرور فقط ثم يتم ارسال البيانات الي خوادم سناب شات للتأكد منها إذا كانت صحيح او لا من خلال تطبيق Burp Suite راح نشوف البيانات قبل ارسالها للشركة ثم نقرر نكمل او نغلق الارسال او نعدل على البيانات

II7MAD99@GMAIL.COM 26 Oct 2021

اكيد وصلت لك الفكرة صح؟ طيب خلينا نثبت تطبيق Burp Suite على الكمبيوتر الخاص فينا ..

نروح الي محرك البحث قوقل ونكتب: burp suite install
وندخل على الموقع المحدد بصوره



II7MAD99@GMAIL.COM 26 Oct 2021

ثم ننزل نضغط على:

PROFESSIONAL COMMUNITY

Downloading and installing Burp Suite

Last updated: August 6, 2021 **Read time:** 2 Minutes

The process for downloading Burp Suite is slightly different depending on whether you are installing Burp Suite Professional or Burp Suite Community Edition.

Downloading Burp Suite Professional

You can download the installer for any version of Burp Suite from the Releases page without needing to log in. This is useful if you already have a license key.

If you don't have a license key yet, we recommend registering for a free trial or purchasing a license first. Once you have an account, you can download both your license key and the latest version of Burp Suite for your required platform (Windows, MacOS, or Linux) from your account page.

Note that you can also choose to download Burp Suite as a JAR file and launch it directly from the command line instead of using one of the native platform installers.

Downloading Burp Suite Community Edition

To download the free community edition of Burp Suite, go to the Download Burp Suite Community Edition page. You can then proceed to installing Burp Suite.

ثم اضغط على DOWNLOAD

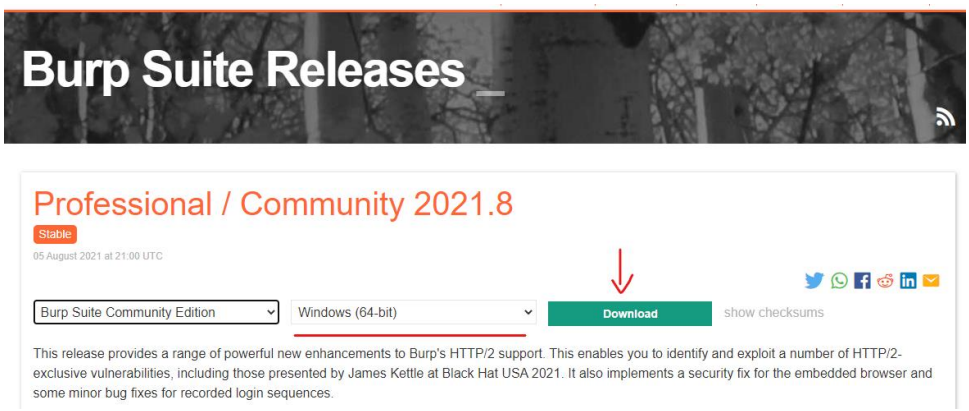
Burp Suite Community Edition

Start your web security testing journey for free - download our essential manual toolkit.

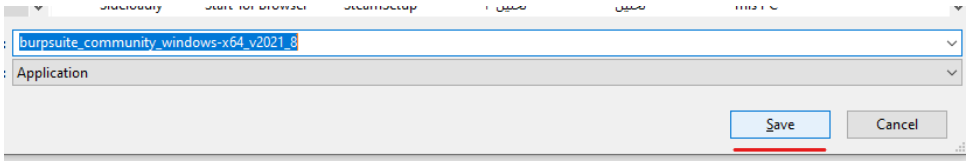
DOWNLOAD TRY PRO FOR FREE

II7MAD99@GMAIL.COM 26 Oct 2021

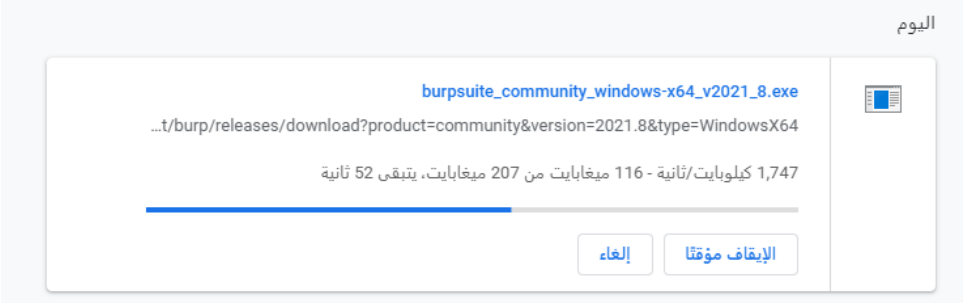
ثم اختار نوع جهازك ثم DOWNLOAD



ثم اختار مكان الحفظ وضغط Save

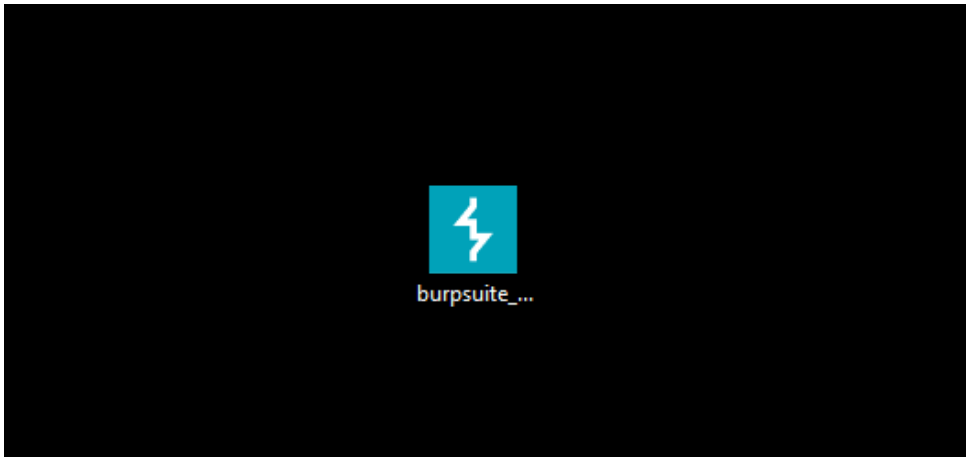


جاري تنزيل البرنامج

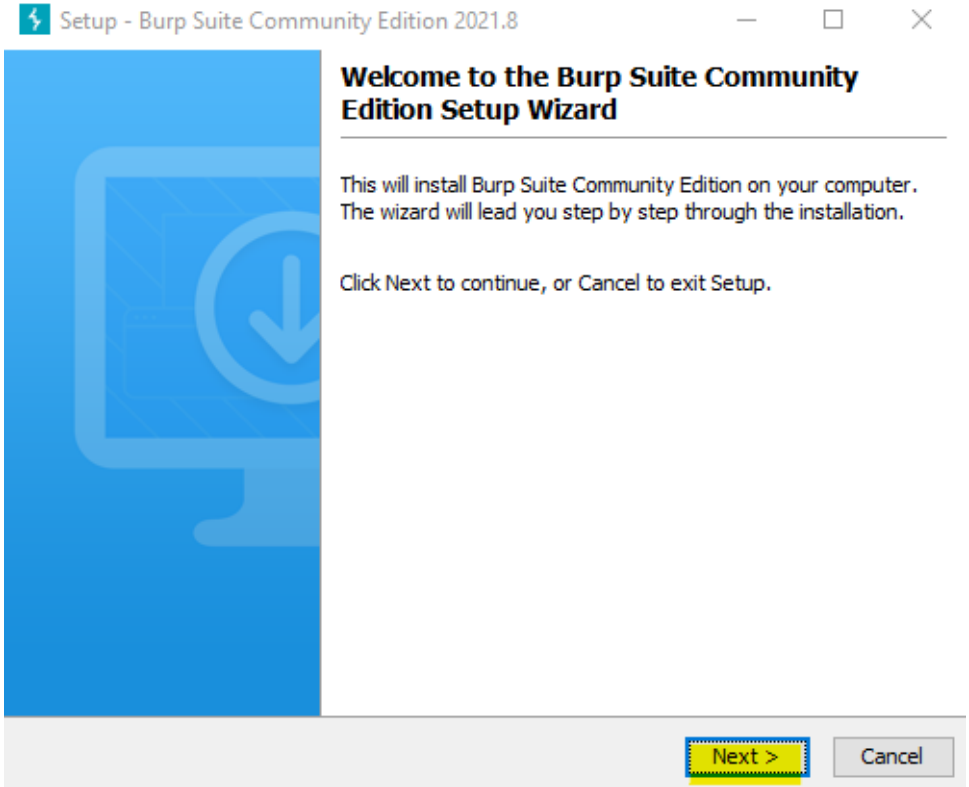


II7MAD99@GMAIL.COM 26 Oct 2021

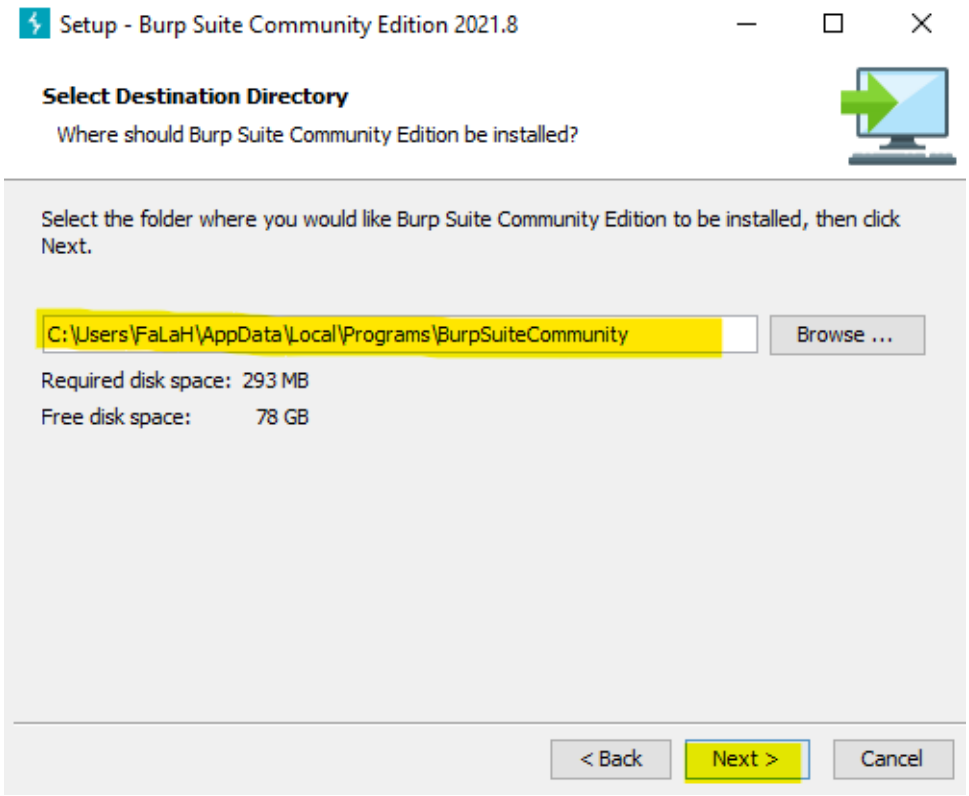
تم تحميله بنجاح على سطح المكتب

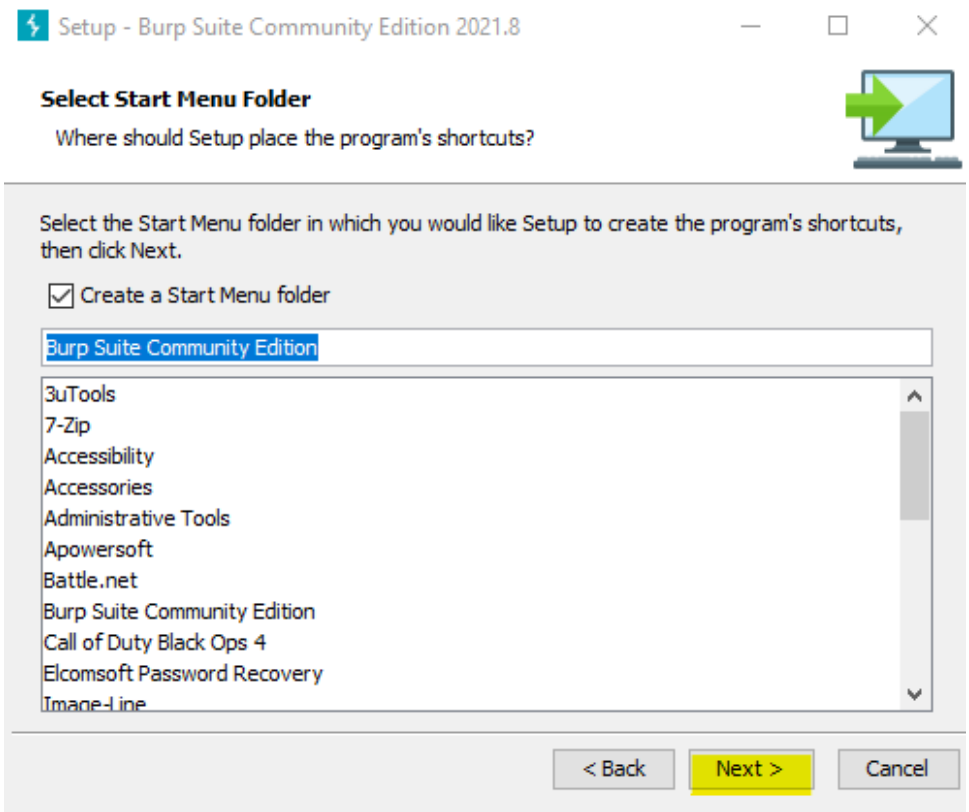


اضغط عليه وتابع خطوات تنصيبه

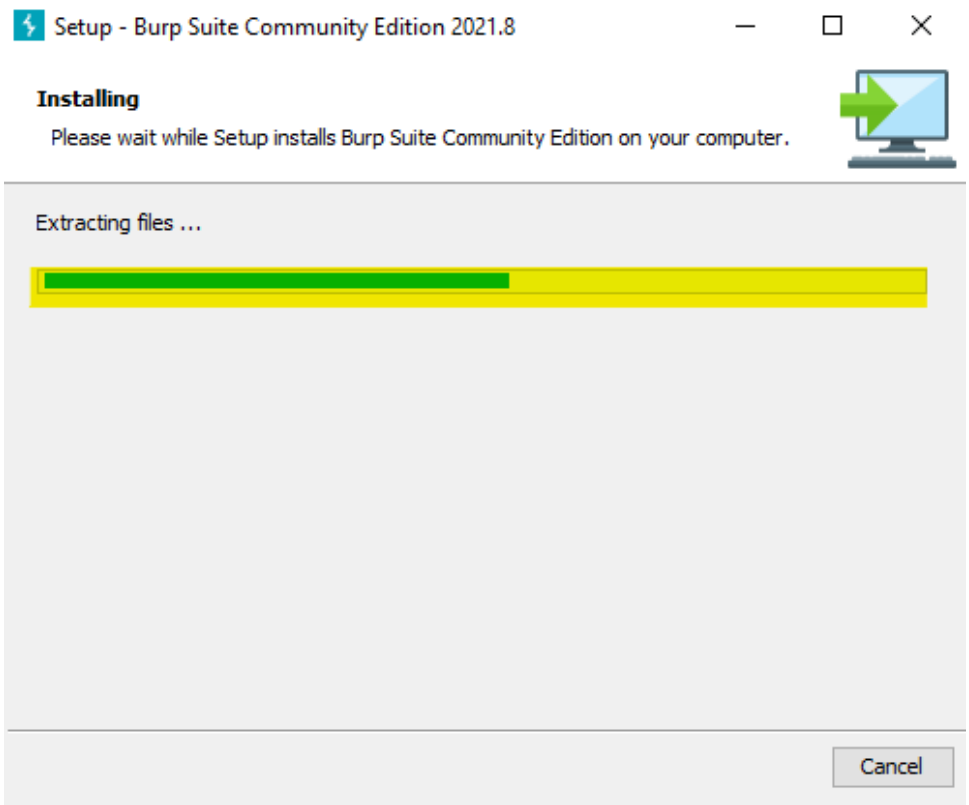


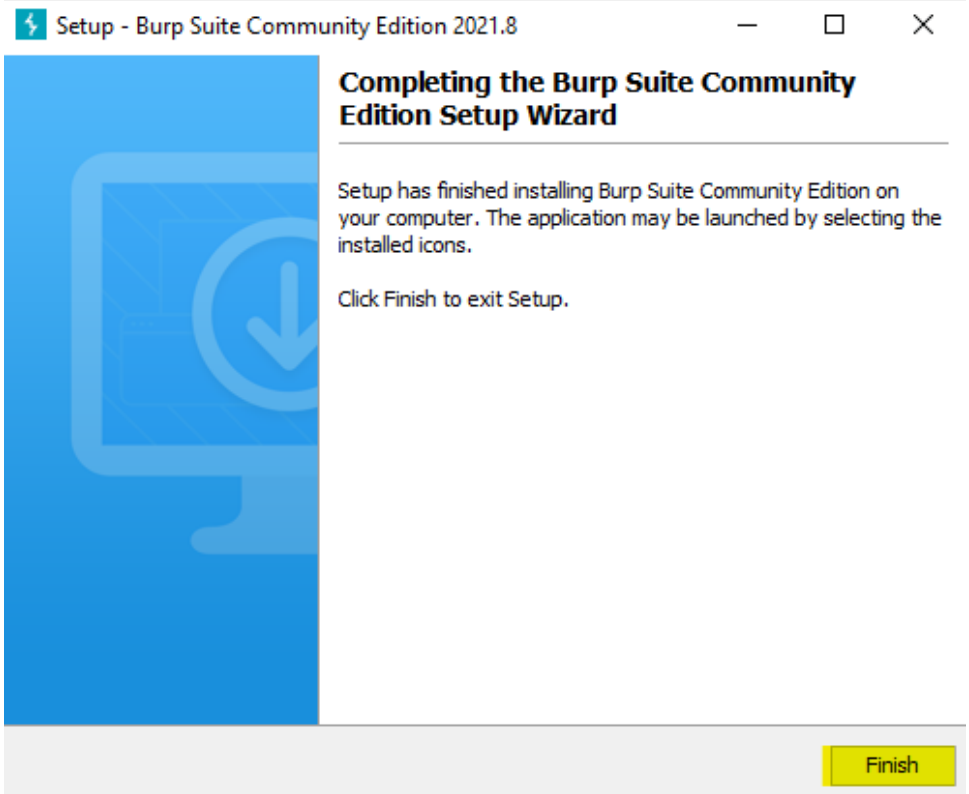
II7MAD99@GMAIL.COM 26 Oct 2021



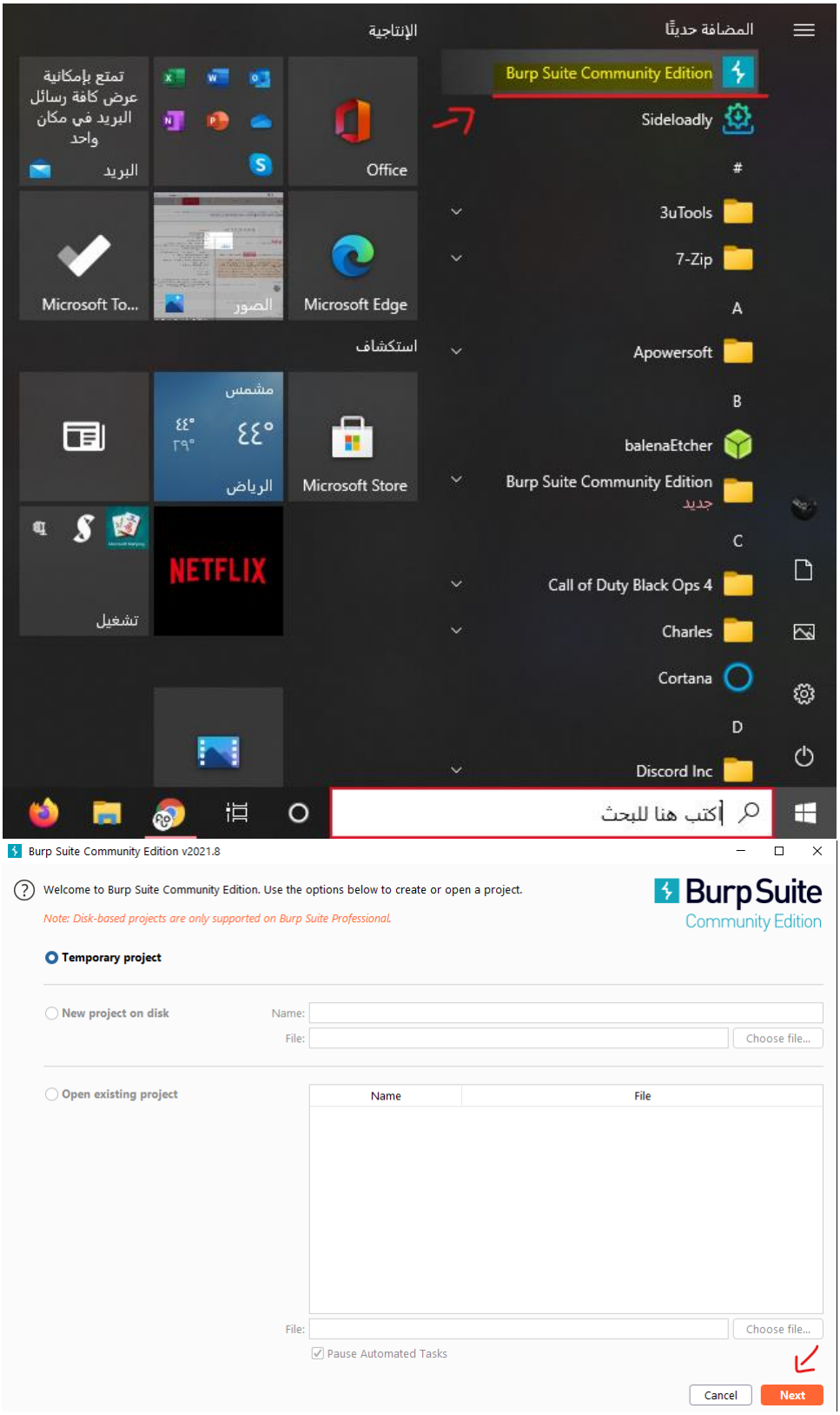


II7MAD99@GMAIL.COM 26 Oct 2021

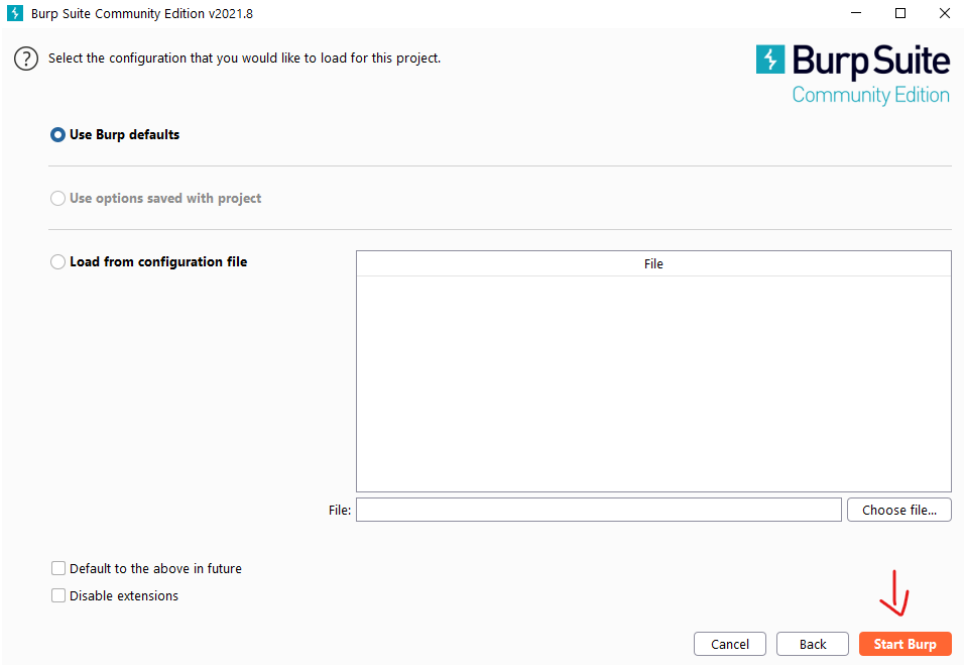




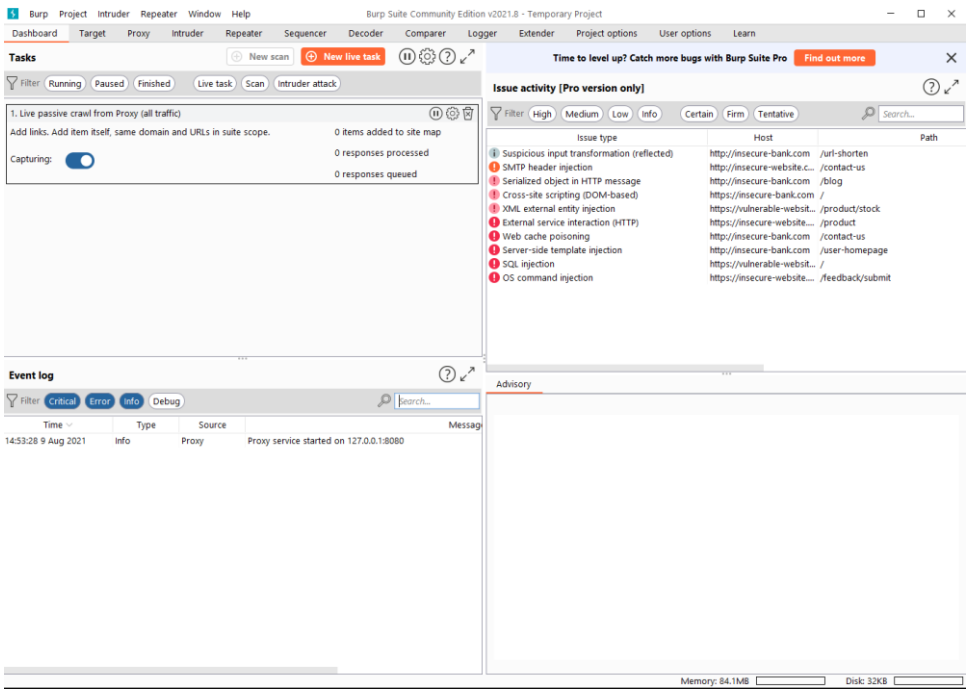
II7MAD99@GMAIL.COM 26 Oct 2021



II7MAD99@GMAIL.COM 26 Oct 2021

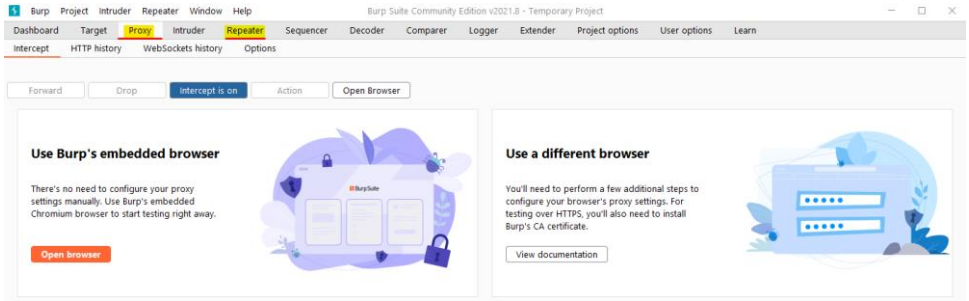


تم تشغيل Burp Suite بنجاح



II7MAD99@GMAIL.COM 26 Oct 2021

في الشريط العلوي يوجد اقسام متعددة
فقط نحتاج قسم Proxy و Repeater في كتابنا



عند الضغط على قسم Proxy سوف تشاهد اقسام تابعه للقسم منها:

- **Intercept**
- **HTTP history**
- **WebSockets history**
- **Options**

في القسم Intercept راح تشوف الطلبات التطبيق
من خلالها تقدر تعدل على أي طلب قبل ارساله

في القسم HTTP history راح تشوف جميع الطلبات التي تم استقبالها من التطبيق ورسالها للخوادم مثل الهوست و الايبي واللينك وغيرها..

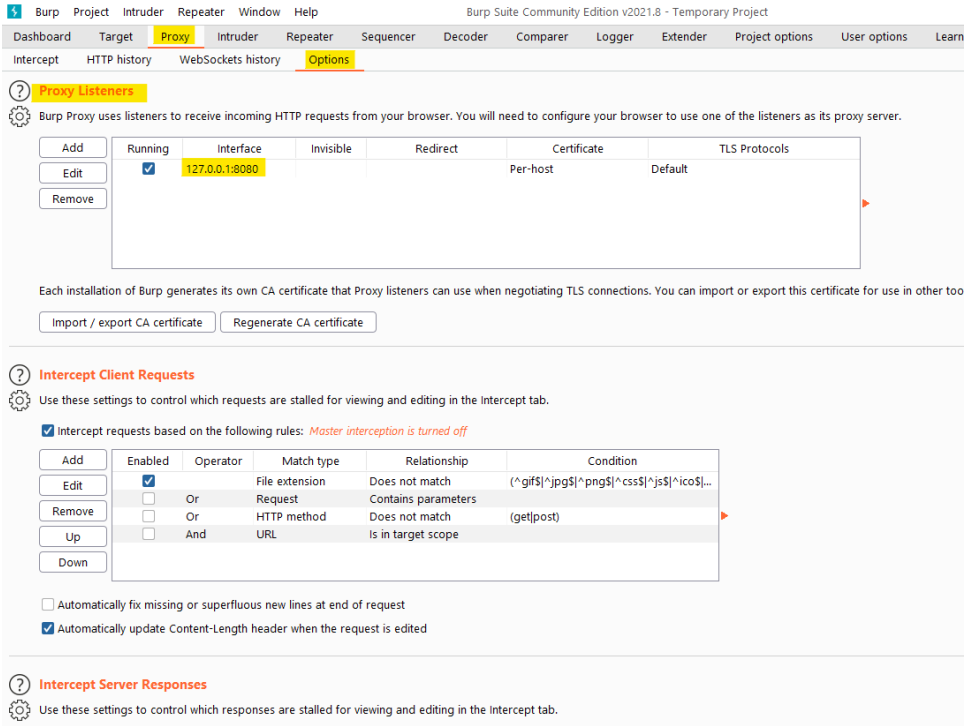
في WebSockets history غالبا ماراح نحتاجه ابد لكن مجبور أوضح لك ماذا يعني باختصار هو إعداد الاتصال ودورات استجابة متكررة للطلب، على بروتوكول HTTP TCP وبنسبه لنا غير مفيد

II7MAD99@GMAIL.COM 26 Oct 2021

في القسم Options مهم بنسبه لنا نقدر من خلاله نربط اجهزتنا من خلال القسم المذكور مثل اضافه هاتف متصل معنا بنفس الشبكة من خلال ip

عشان نقدر نفحص التطبيقات الموجودة على الهاتف

للتوضيح:

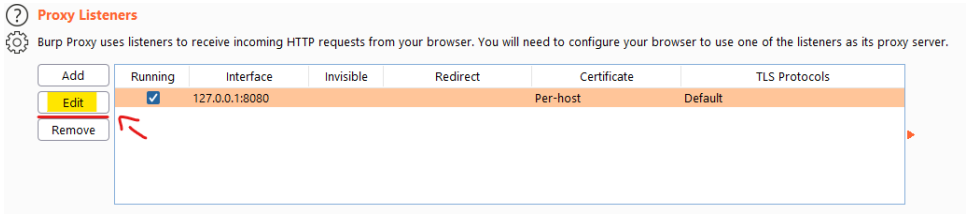


تشاهد الايي ١٢٧,٠,٠,١ وهذا الايي جهاز الكمبيوتر الخاص بنا نحتاج نغيره الي الايي الخاص في هواتفنا الايفون المتصلة بنفس شبكة الكمبيوتر

II7MAD99@GMAIL.COM 26 Oct 2021

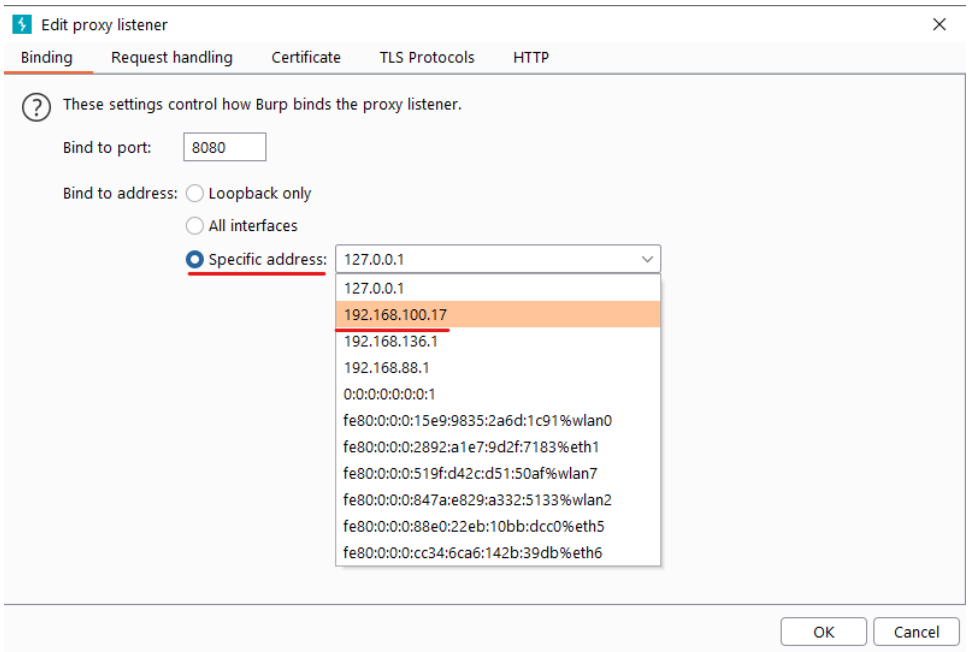
كيف يتم تغيره؟

نضغط علي الايبي ثم نذهب الي خيار: Edit



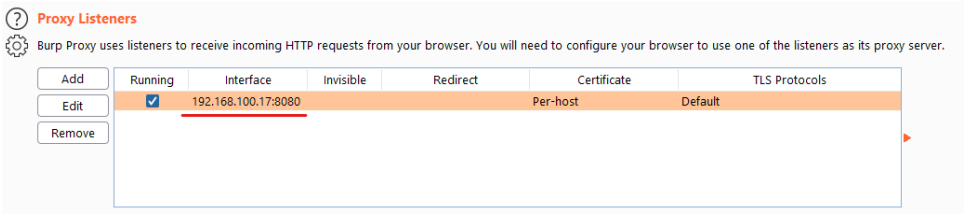
ثم نختار الايبي الي تحت ١٢٧,٠,٠,١

إذا لم يتصل معك بعد ربطه في الايفون جرب ايبي اخر
للمعلومة ال - Ip الموجود بصوره يختلف من جهاز الي جهاز اخر



II7MAD99@GMAIL.COM 26 Oct 2021

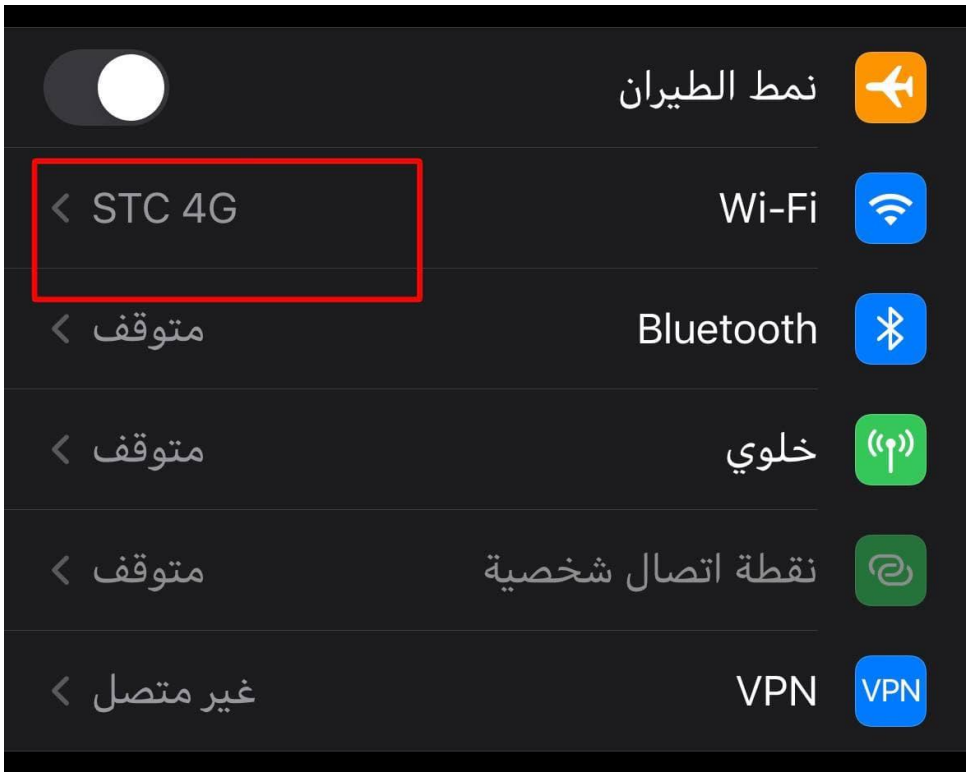
ثم ok



سوف تلاحظ تم تغيره الي الايبي الي اخترناه
الان نحتاج نذهب الي اعدادات الايفون الي راح نفحص التطبيقات منه

ونكتب الايبي الي حطينا في برنامج Burp Suite

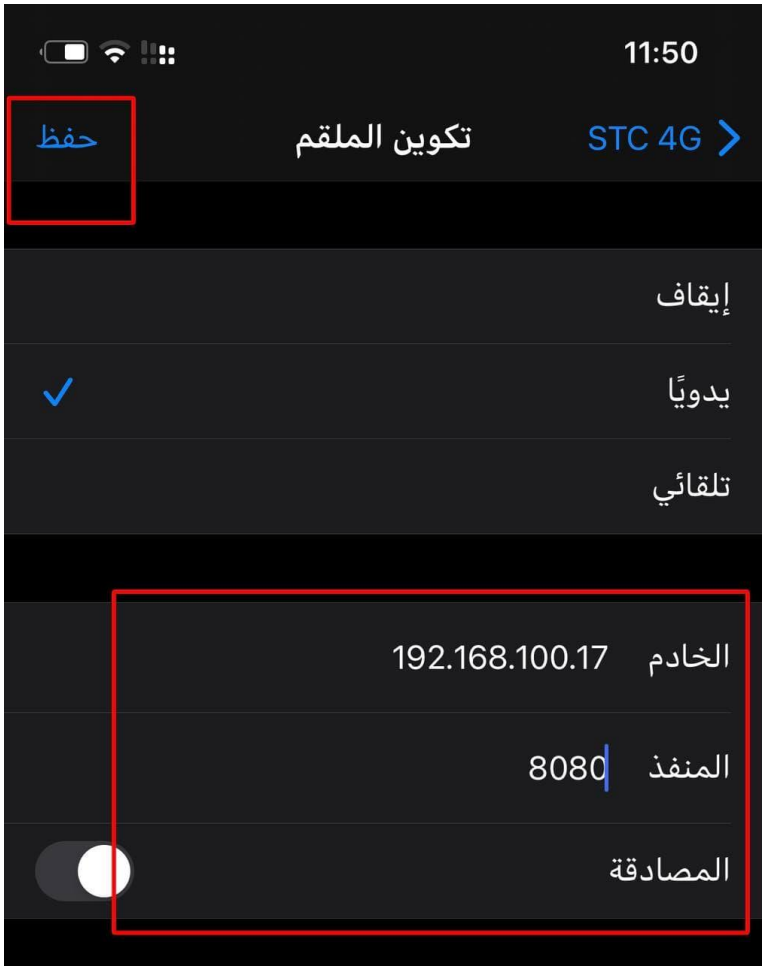
تابع الخطوات



II7MAD99@GMAIL.COM 26 Oct 2021

II7MAD99@GMAIL.COM 26 Oct 2021

نكتب الايبي الي حطيناه في برنامج Burp Suite مع المنفذ ٨٠٨٠ ثم حفظ

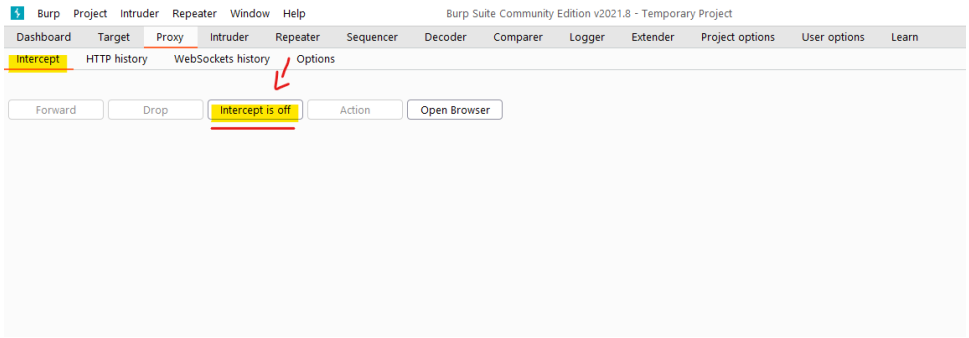


II7MAD99@GMAIL.COM 26 Oct 2021

الان نرجع الي برنامج Burp Suite

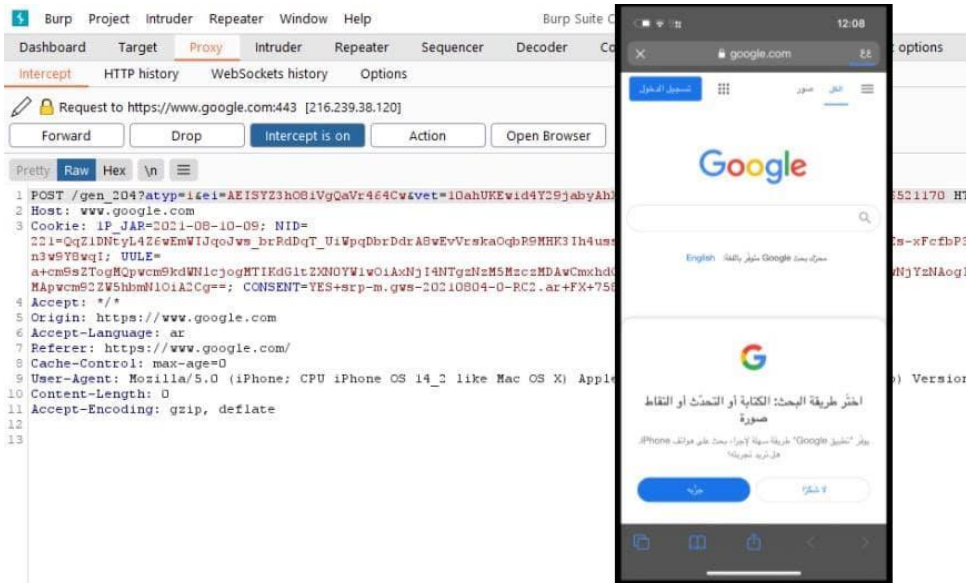
ونذهب الي خيار Intercept بنفس قسم Proxy

ونفعل خيار Intercept is off الي Intercept is on

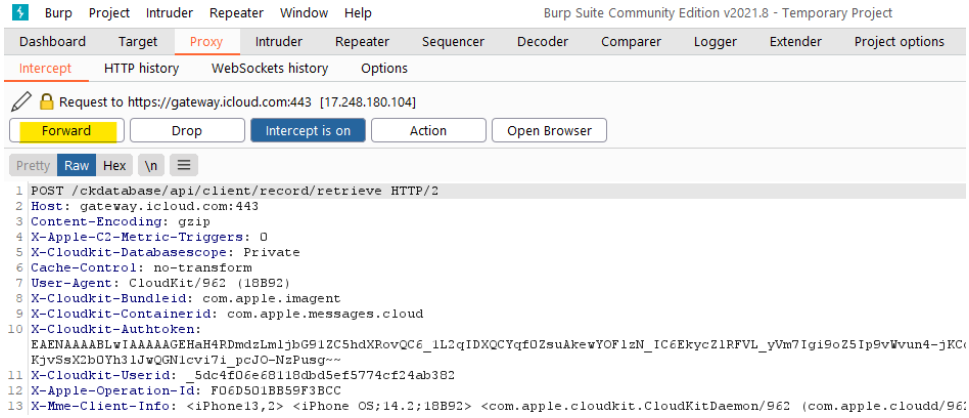


الان لو نذهب الي متصفح Safari في الايفون
وندخل الي Google راح تلاحظ الطلب طلع في برنامج Burp Suite

II7MAD99@GMAIL.COM 26 Oct 2021



اذا حاب تشوف الطلب الي بعده اضغط على : Forward



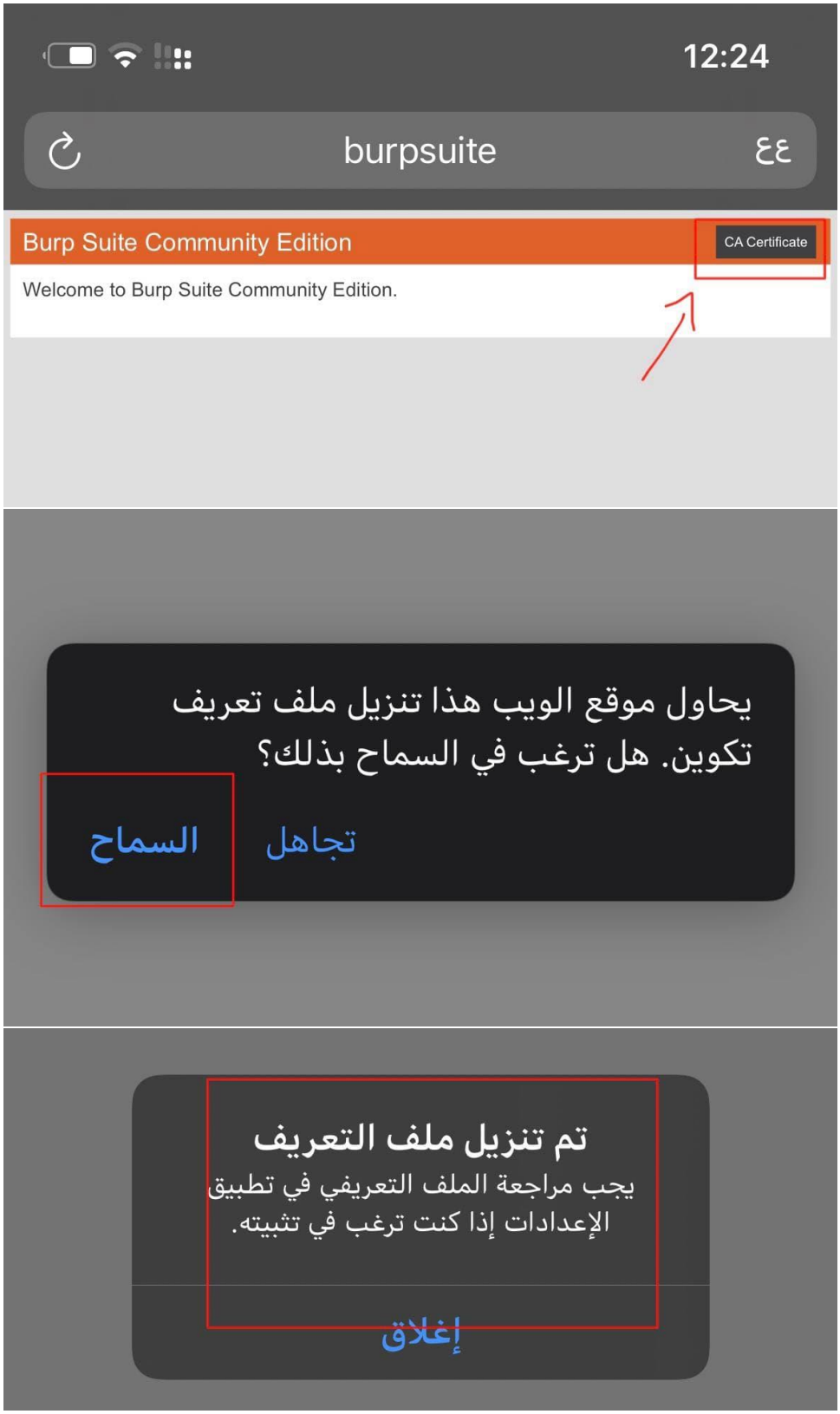
الان نحتاج ربط شهادة Burp Suite في الايفون حقنا عشان نقدر نفحص التطبيقات بدون مشاكل

نذهب الي متصفح Safari ونكتب الرابط التالي :

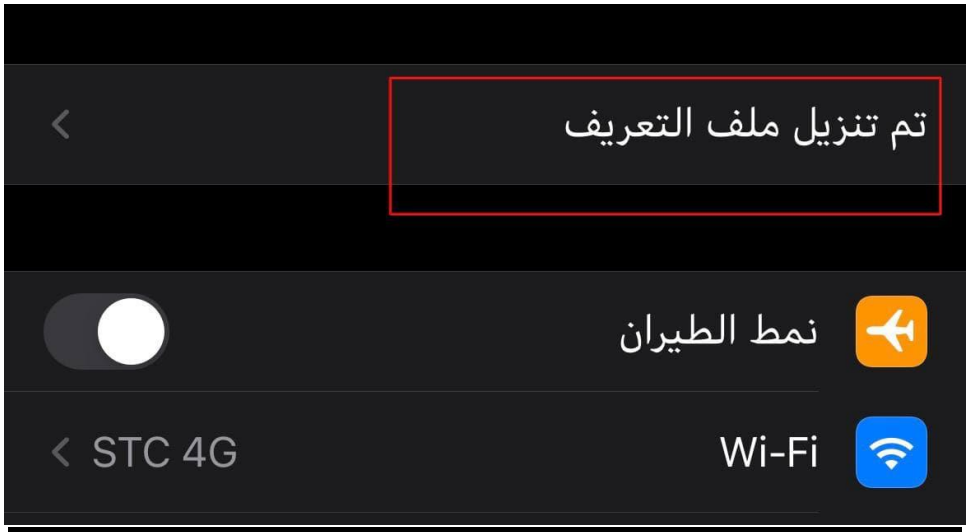
http://burpsuite

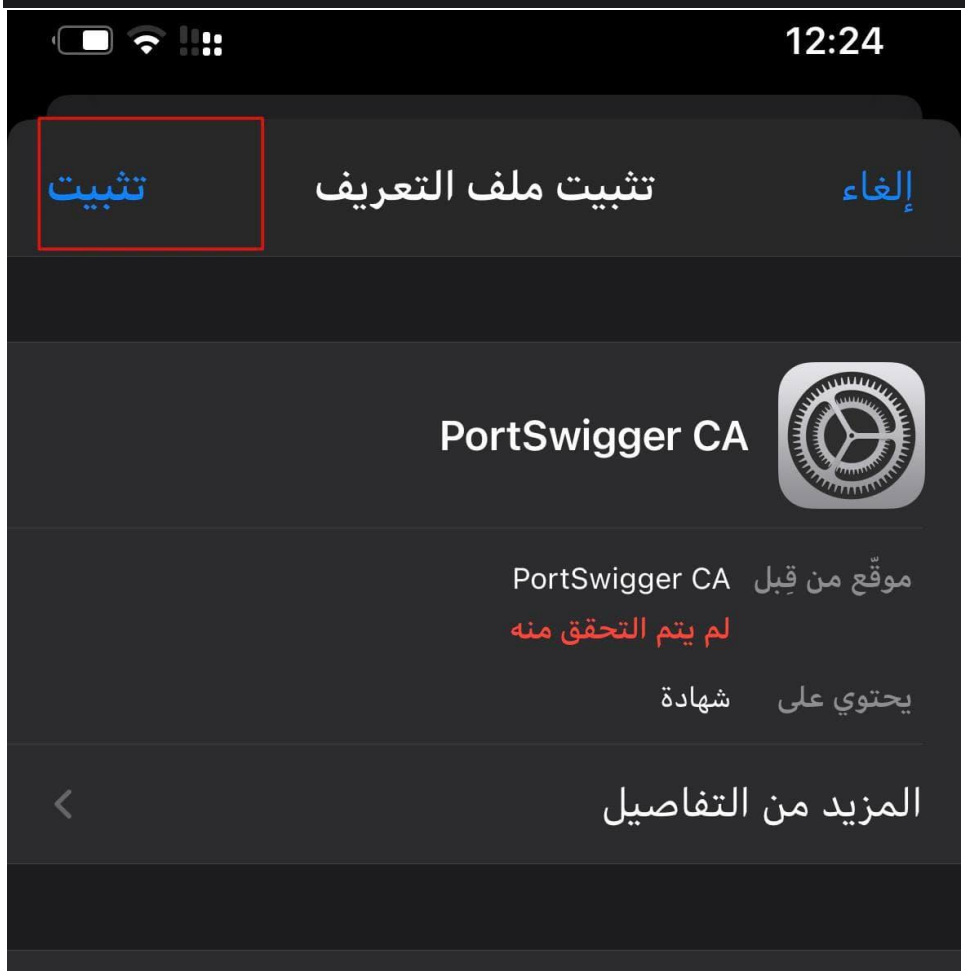
II7MAD99@GMAIL.COM 26 Oct 2021

ثم تابع الخطوات التاليه :

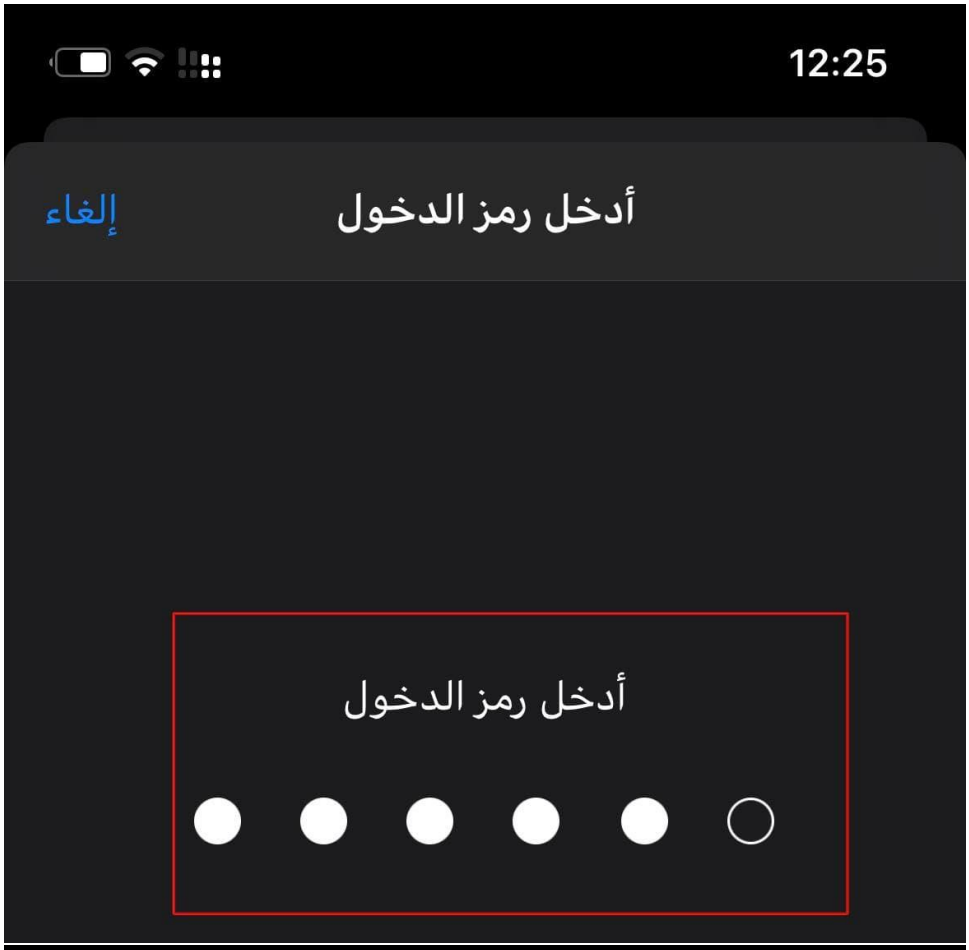


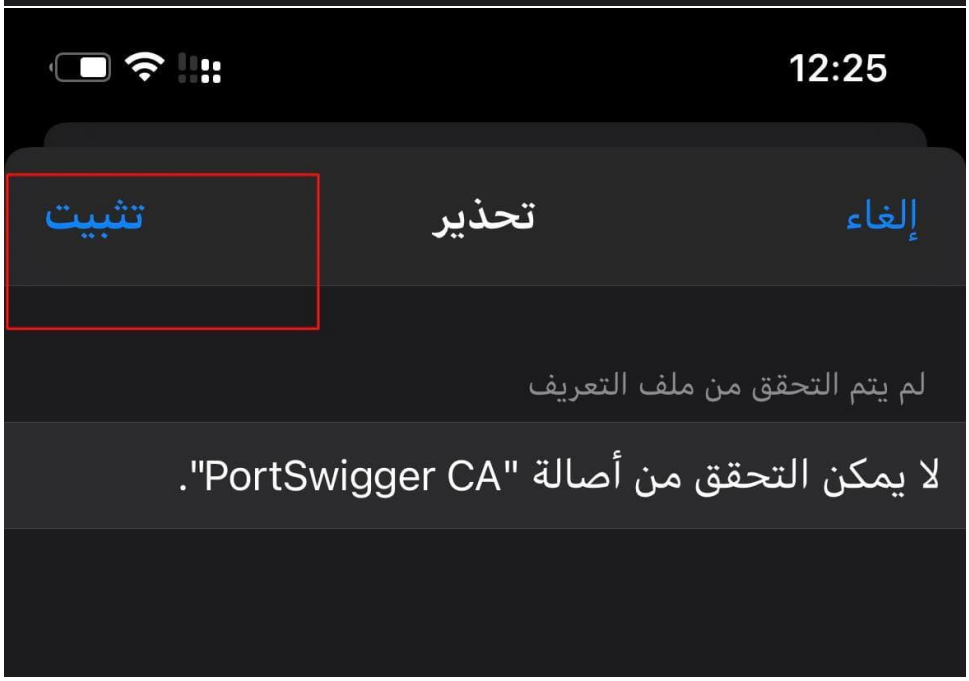
II7MAD99@GMAIL.COM 26 Oct 2021





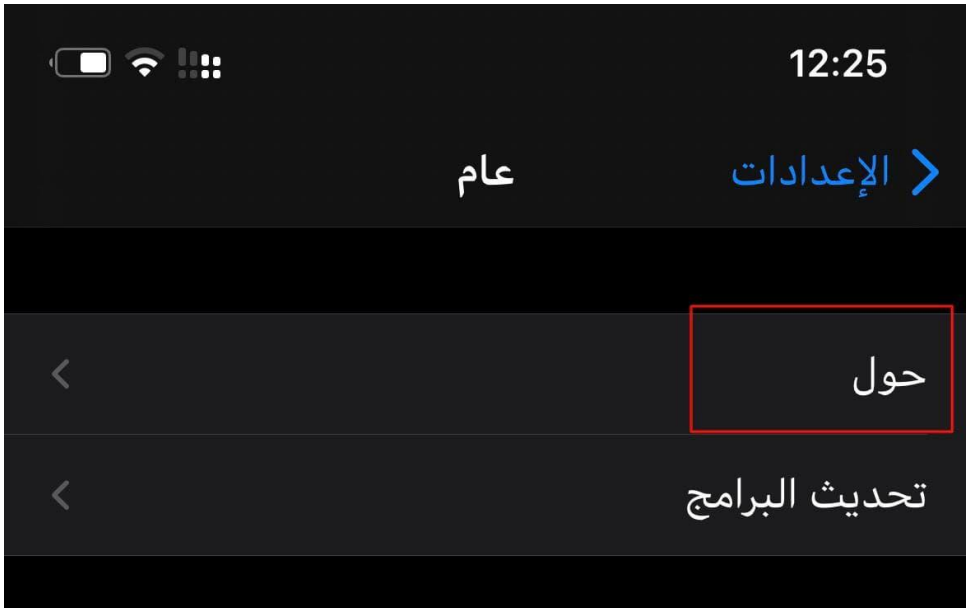
II7MAD99@GMAIL.COM 26 Oct 2021





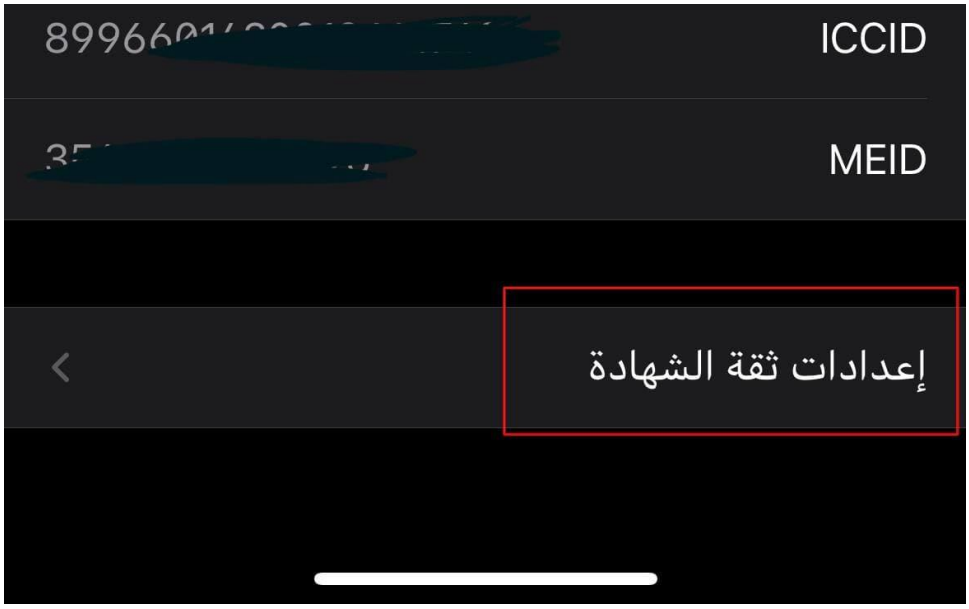
II7MAD99@GMAIL.COM 26 Oct 2021

ثم ارجع الي الاعدادات ثم اذهب الي عام ثم حول:

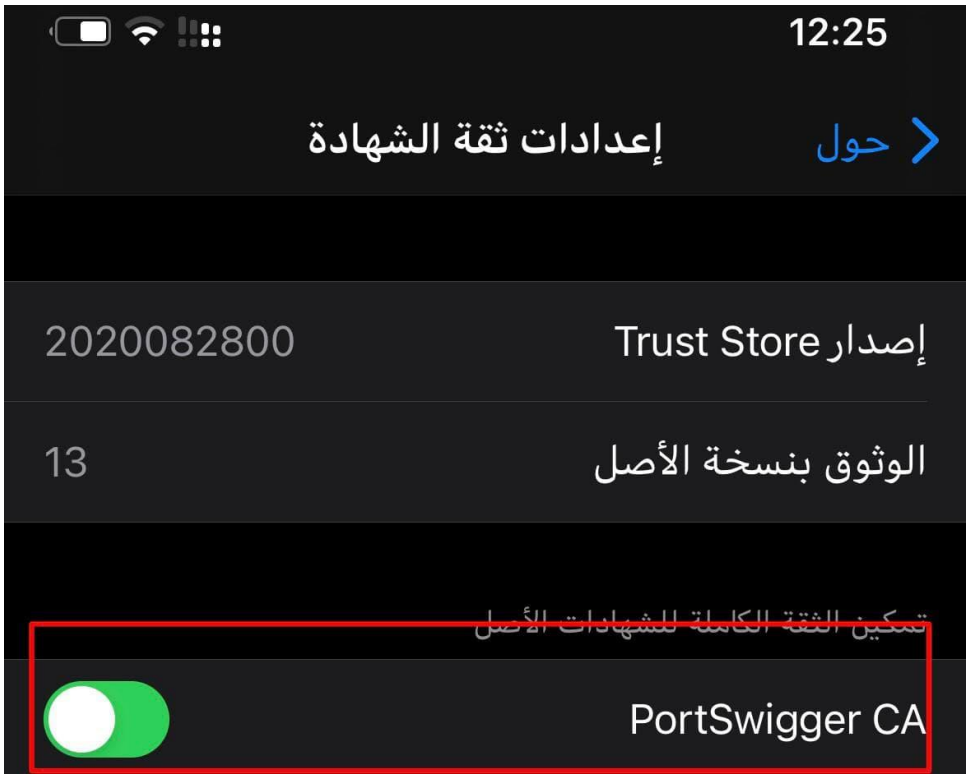


II7MAD99@GMAIL.COM 26 Oct 2021

انزل الي نهاية الاعدادات عند خيار الوثوق في ثقة الشهادة



فعل خيار الوثوق في الشهادة مثل الصورة :



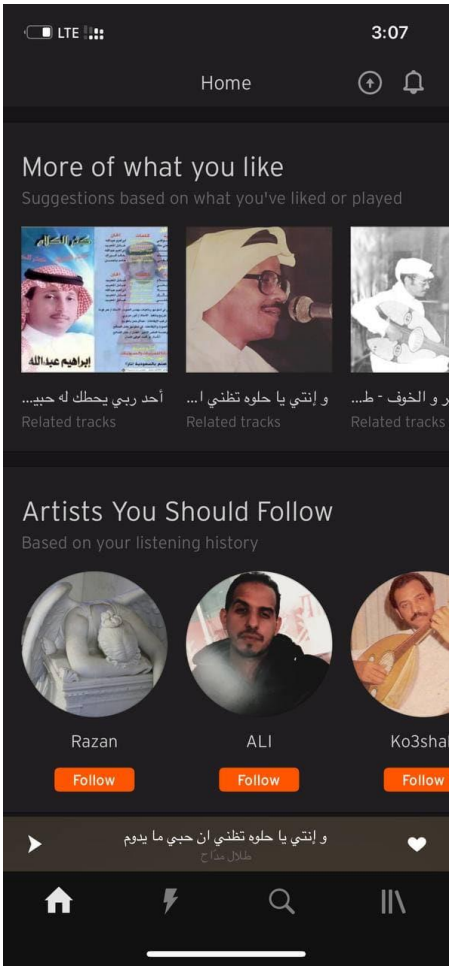
II7MAD99@GMAIL.COM 26 Oct 2021

الان تم ربط الشهادة في الهاتف بنجاح وتستطيع فحص التطبيقات كامله بدون مشاكل

الان نريد نفحص تطبيق SoundCloud للتجربة

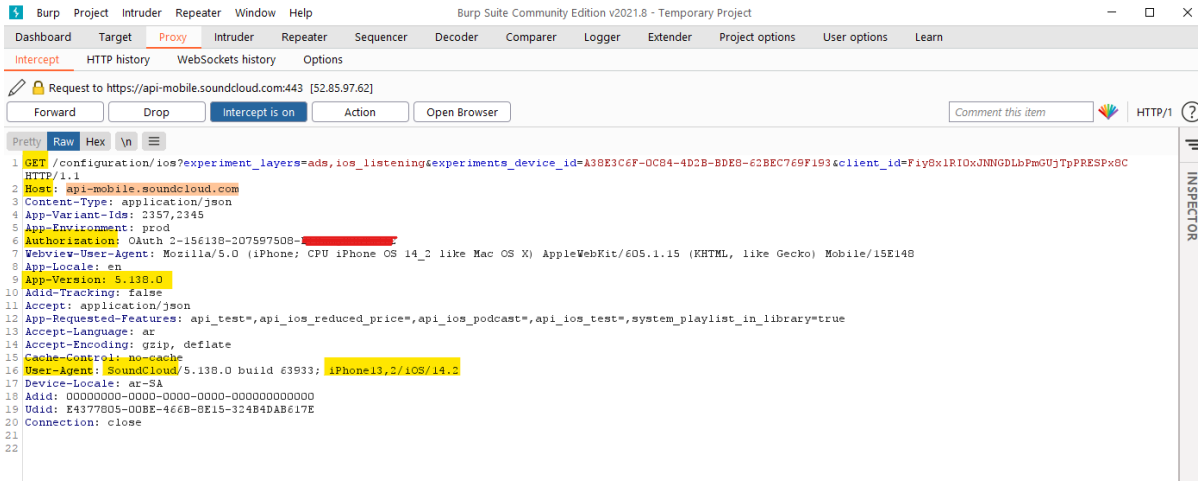
- نتأكد مفعلين خيار Intercept is on من Burp Suite
- نتأكد رابطين جوالنا في البرنامج Burp Suite
- نتأكد من اغلاق جميع التطبيقات من الخلفية ونجعل فقط تطبيق SoundCloud

الان ندخل الي تطبيق : SoundCloud



II7MAD99@GMAIL.COM 26 Oct 2021

نشاهد عند الدخول طلع لنا طلب الاتصال في Burp Suite

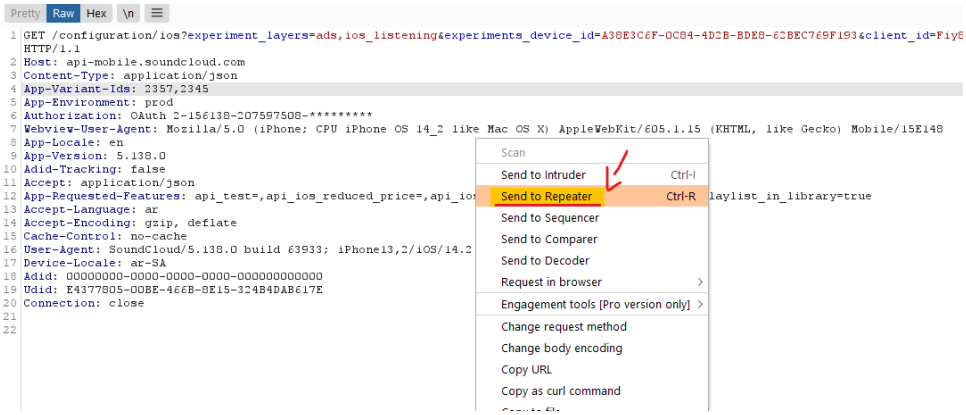


عندك في الطلب طلع لنا نوع الصفحة والهوست ونوع الإصدار وغيرها

GET
configuration/ios?experiment_layers=ads,ios_listening&experiments_device_id=A38E3C/6F-0C84-4D2B-BDE8-62BEC769F193&client_id=Fiy8xlRI0xJNNGDLbPmGUjTpPRESPx8C
HTTP/1.1
api-mobile.soundcloud.com :Host
application/json :Content-Type
2357,2345 :App-Variant-Ids
prod :App-Environment
OAuth 2-156138-207597508 :Authorization
en :App-Locale
5.138.0 :App-Version
false :Adid-Tracking
application/json :Accept
:App-Requested-Features
system_playlist_in_libr,=api_ios_test,=api_ios_podcast,=api_ios_reduced_price,=api_test
ary=true
ar :Accept-Language
deflate ,gzip :Accept-Encoding
no-cache :Cache-Control
SoundCloud/5.138.0 build 63933; iPhone13,2/iOS/14.2 :User-Agent
ar-SA :Device-Locale
00000000-0000-0000-0000-000000000000 :Adid
E4377805-00BE-466B-8E15-324B4DAB617E :Udid

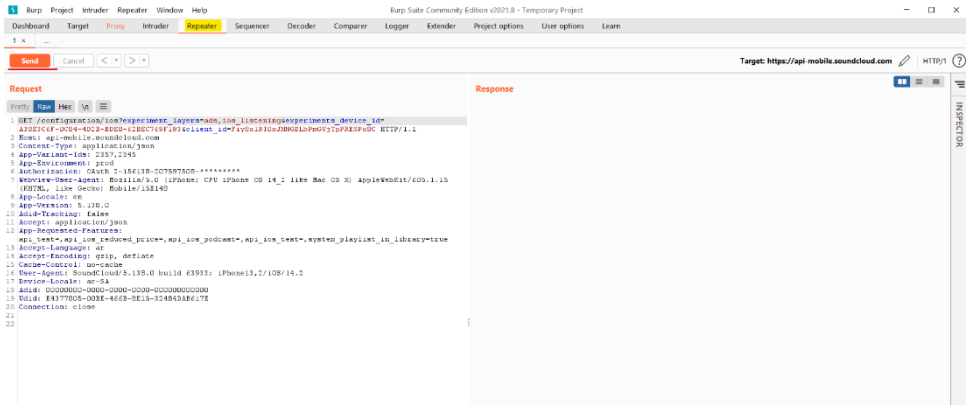
II7MAD99@GMAIL.COM 26 Oct 2021

نضغط كليك يمين في الماوس ونختار كلمة : Send to Repeater

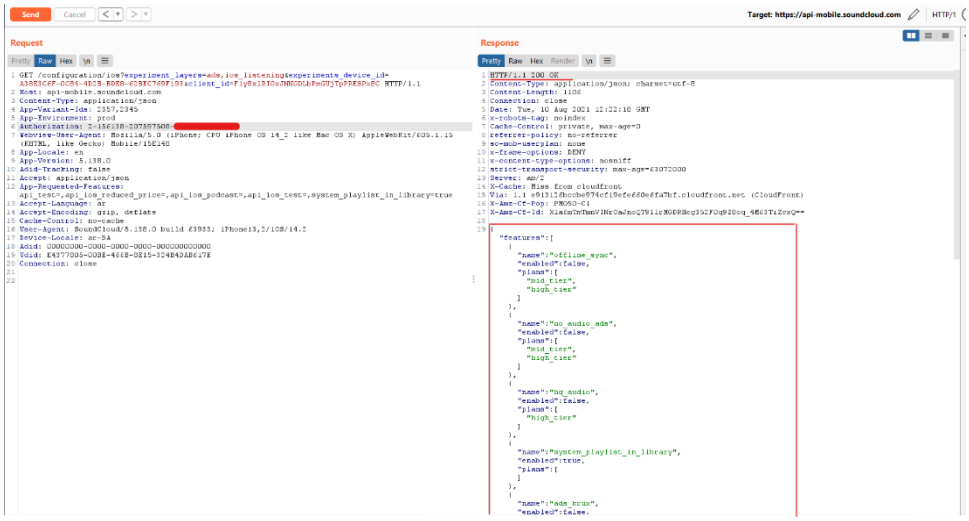


راح يوجهنا الي قسم Repeater عشان نشوف رد السيرفر

نضغط Send



السيرفر رد علينا :

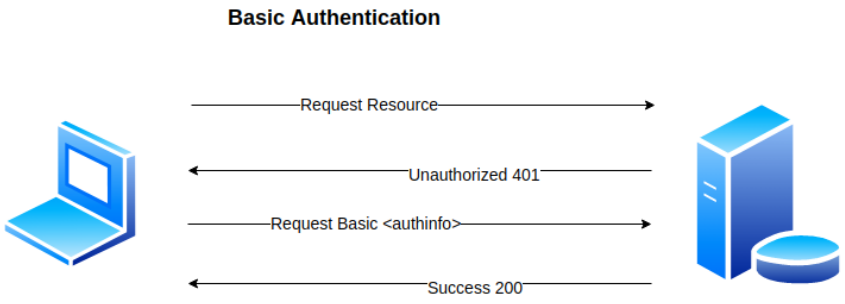


II7MAD99@GMAIL.COM 26 Oct 2021

الرد كان HTTP 200 ok وطلع لنا البيانات

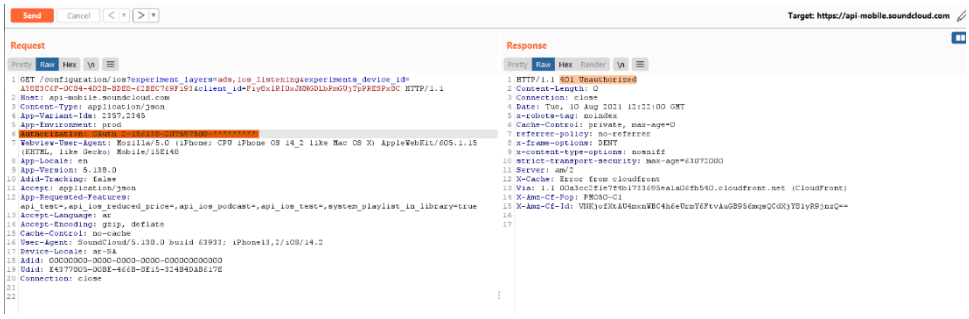
يعني امورنا الحين طيبه بس لو طلع لك Unauthorized 401 ؟
يعني غير مصرح لك الوصول للبيانات من قبل السيرفر

والسبب غالبا يكون من Authorization في بيانات الركويست



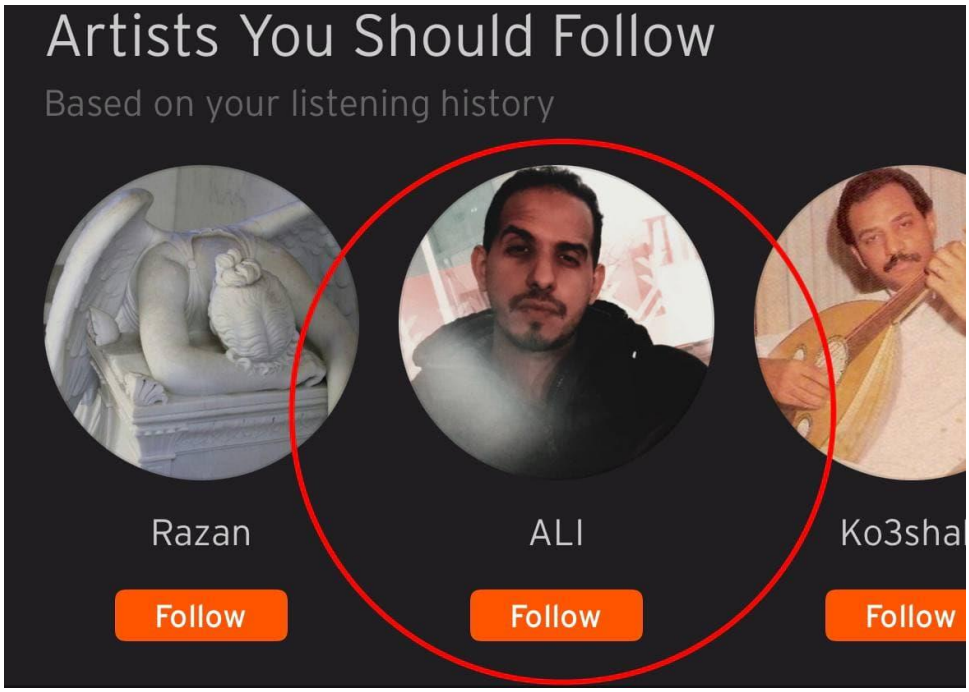
ويعني Authorization مفتاح لحسابك بدال كلمة السر
اذا تم العبث في الطلب راح يكون رد السيرفر 401
عشان أوضح لك عدلت Authorization

وكان الرد 401 غير مفوض لي



II7MAD99@GMAIL.COM 26 Oct 2021

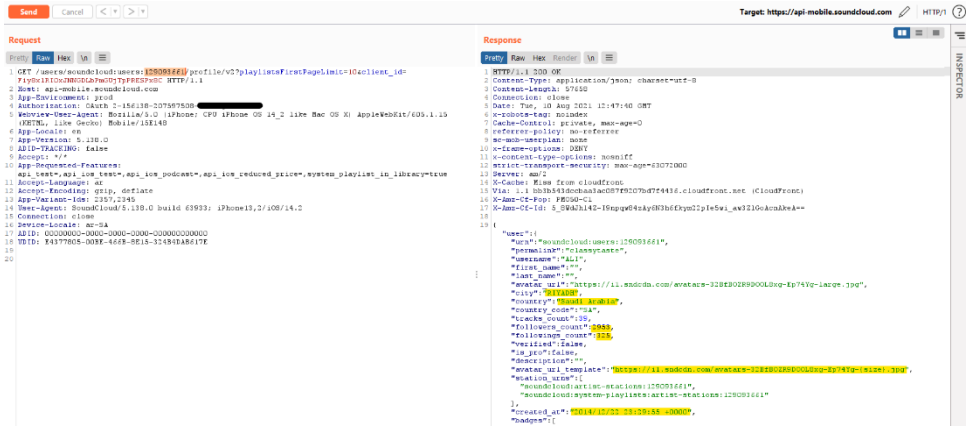
الان لو نرجع للتطبيق ونضغط على ملف التعريف أحد الحسابات مثال حساب ALI



طلع لنا في : Burp Suite
User:129093661 وهو معرف حساب ALI

II7MAD99@GMAIL.COM 26 Oct 2021

نضغط كليك يمين في الماوس ونختار كلمة : Send to Repeater
مثل ما تعدونا في السابق عشان نشوف البيانات الحساب



الرد كان 200 وجاب لي بيانات الحساب بدون مشاكل

us","classytaste":"permalink","soundcloud:users:129093661":"urn"}:"{"user
https://i1.sndc":"avatar_url","":"last_name","":"first_name","ALI":"ername
dn.com/avatars-32BfBOZR9DOOL8xg-Ep74Yg-
Saudi ":"country","RIYADH":"city","large.jpg
fol",2953:"followers_count",39:"tracks_count","SA":"country_code","Arabia
avatar_u","":"description",false:"is_pro",false:"verified",325:"lowings_count
-https://i1.sndcdn.com/avatars-32BfBOZR9DOOL8xg-Ep74Yg":"rl_template
soundcloud:artist-"]:"station_urns","jpg.{size}
soundcloud:system-playlists:artist-","stations:129093661
0000"+ 2014/12/22 23:29:55":"created_at",["stations:129093661

- مثل المنطقة المملكة العربية السعودية
- صورة البروفايل
- تاريخ انشاء الحساب
- وعدد المتابعين والي يتابعهم

II7MAD99@GMAIL.COM 26 Oct 2021

طيب الحين جربنا على أحد البرامج بشكل تجريبي لو بغينا نجرب على تطبيق أكثر شهره مثل Twitter ونستخرج بعض اتصالاته وطلباته
نحتاج أولا جلبريك مثل ما ذكرت لك سابقا وطريقة تثبيت الجلبريك موجودة شروحات له في كل مكان مثل اليوتيوب او الانترنت

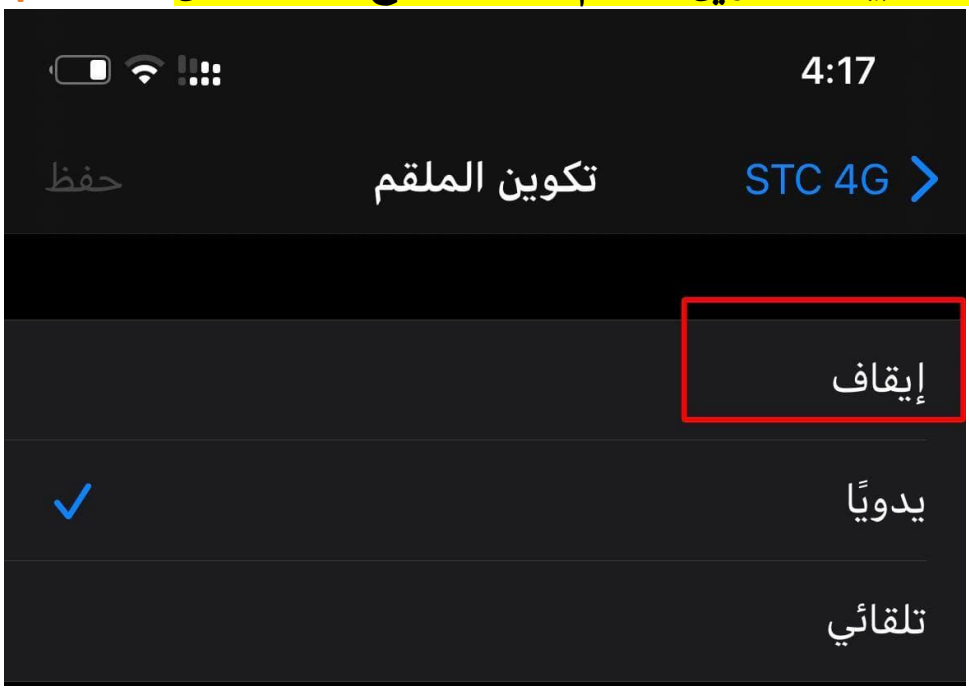
ما يهم نوع الجلبريك اذا كان unc0ver او غيره المهم تثبيت جلبريك بجهازك

١. نحتاج أداة SSLBypass - عشان نتجاوز حماية التطبيقات
٢. نحتاج أداة AppStore - عشان نقدر نرجع إصدارات التطبيقات

تستطيع تثبيتها من Cydia - تتأكد انها تتوافق مع اصدار جهازك الأدوات يتم ذكر التوافقات من قبل مطورين الأدوات مثل من ios 11/14

اذا ان جهازك أقدم من ios 11 او أحدث من ios 14 وتريد تحميلها سوف تسبب لك مشاكل في الجهاز - وجب التنبيه

لاتنسي قبل إيقاف تكوين الملقم عشان تقطع الاتصال من Burp Suite



II7MAD99@GMAIL.COM 26 Oct 2021

بعد تثبيت الأدوات المطلوبة منك الان

رجع اصدار تطبيق تويتر الي ٨,٦٠ بضغطه مطوله على تنزيل او التحديث من داخل متجر ابل ستور ثم Downgrade

ملاحظه:

اذا ثبت الأدوات ورجعت اصدار التطبيقات ارجع فعل التكوين الملقم وحط الايبي السابق والمنفذ اذا كنت جاهز للفحص

الان جاهزين للفحص ندخل التويتر ثم اضافه حساب جديد

كتبت اسم المستخدم: test_9992

كلمة المرور: aa123123

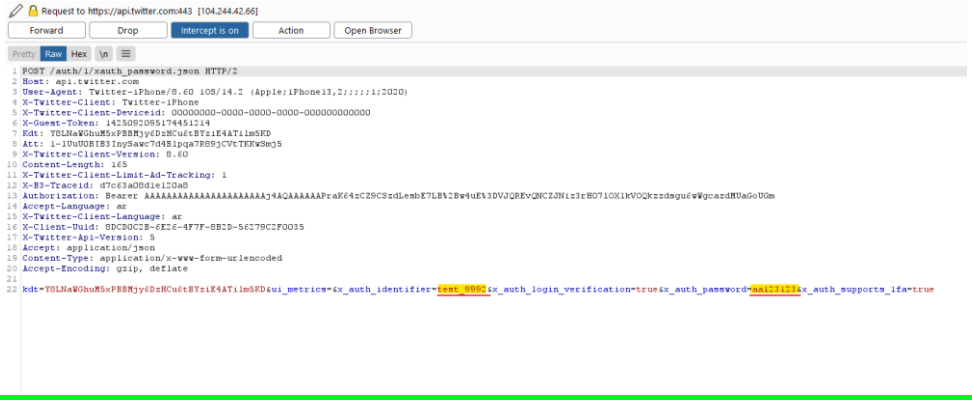
تنبيه لا تستخدم حسابك الأساسي

II7MAD99@GMAIL.COM 26 Oct 2021

ثم ضغطت تسجيل الدخول الان نشاهد طلب تسجيل الدخول في برنامج Burp Suite :

auth/1/xauth_password.json HTTP/2/ POST

api.twitter.com :Host



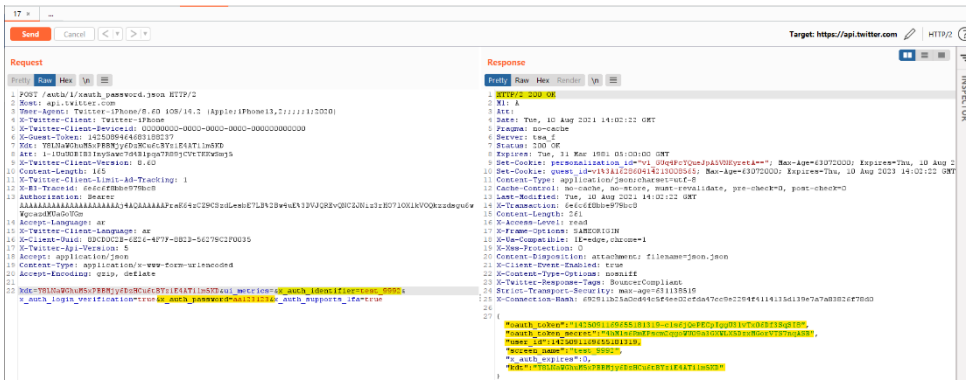
x_auth_identifier=test_9992&x_auth_password=aa123123

اذا طلعت لك البيانات مشفره اغلق التطبيق وحاول مره ثانيه

طلع عندنا في الطلب اسم المستخدم وكلمة المرور الي كتبناها في التطبيق

نضغط كليك يمين في الماوس ونختار كلمة : Send to Repeater

نشوف الرد السيرفر



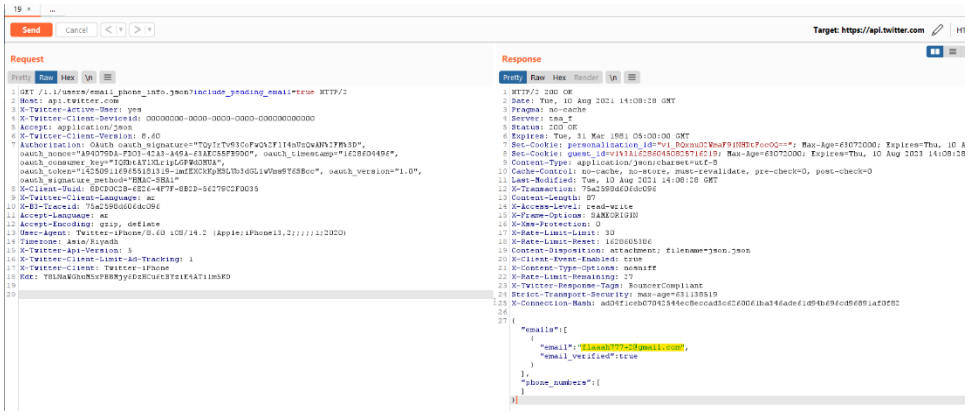
تم تسجيل الدخول بنجاح اذا كان رد السيرفر 401 كلمة المرور خطاء او اسم المستخدم

II7MAD99@GMAIL.COM 26 Oct 2021

كيف نطلع الاميل مع رقم الهاتف من : Burp Suite

نروح الي اعدادات التويتر ثم الحساب
نرجع الي Burp Suite نحصل الطلب طلع لنا:

1.1/users/email_phone_info.json?include_pending_email=true HTTP/2/ GET
api.twitter.com :Host



emails":[{"email":"flaaah777+2@gmail.com","email_verified":true}],"phone_numbers

كما تشاهد طلع لنا الاميل: flaaah777+2@gmail.com

بخصوص رقم الجوال ما طلع لأنه حسابنا بدون رقم جوال

Authorization في التويتر متغير غير ثابت وله وقت معين وينتهي
لا تستطيع فحصه بشكل كامل التويتر يطلب مفاتيح Api للمطورين

راجع المصدر: https://developer.twitter.com/en/docs

سابقا كان تستطيع الاستعلام عن حسابات من نفس حسابك الان لأستطيع تغير كلمة واحد في الطلب اذا حاولت راح يطلع لك 401

II7MAD99@GMAIL.COM 26 Oct 2021

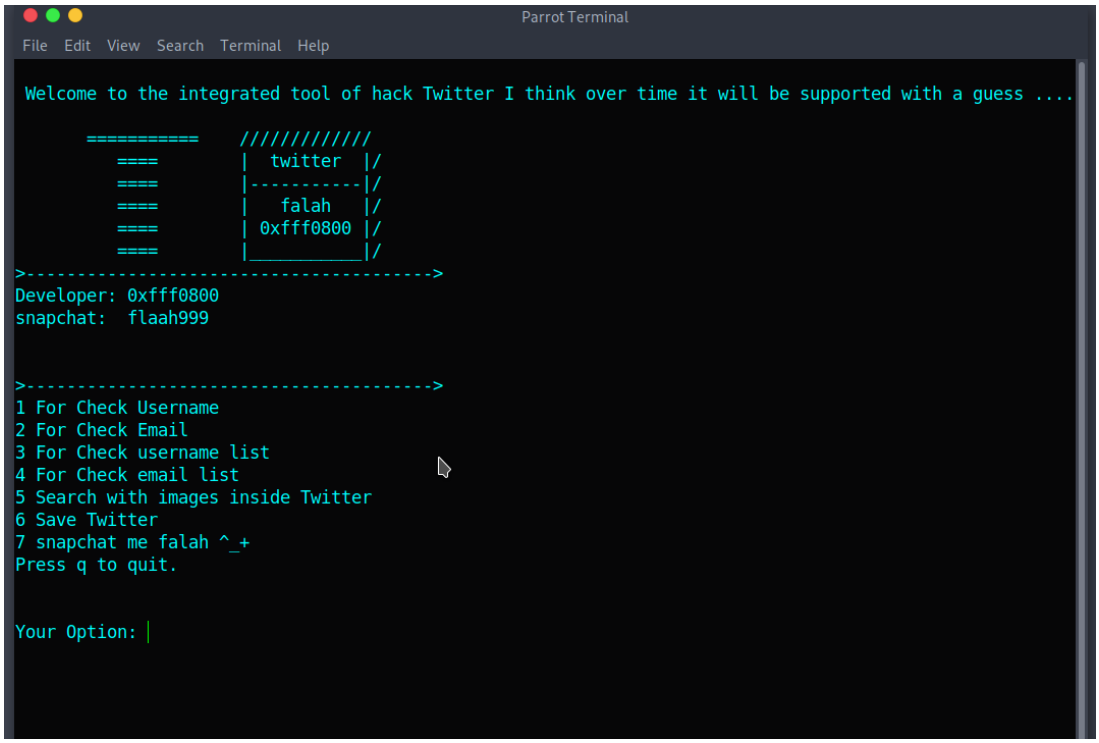
لكن طلب تسجيل الدخول يعمل بدون مشاكل وتستطيع تغير في اسم المستخدم او كلمة المرور من الطلب

إذا بغيت تخمن على حسابات تحتاج sleep لكل 12 تخمينه

التشكير Api / في تطبيق تويتر يكون من انشاء حساب جديد

أداة مبرمجها بنفسي: https://github.com/0xfff0800/hack-Twitter

فائدتها: استعلام عن يوزرات متاحه - استعلام عن اميلات مربوطة وتفيدك بعد تجاوز صفحة تأكيد الاميل



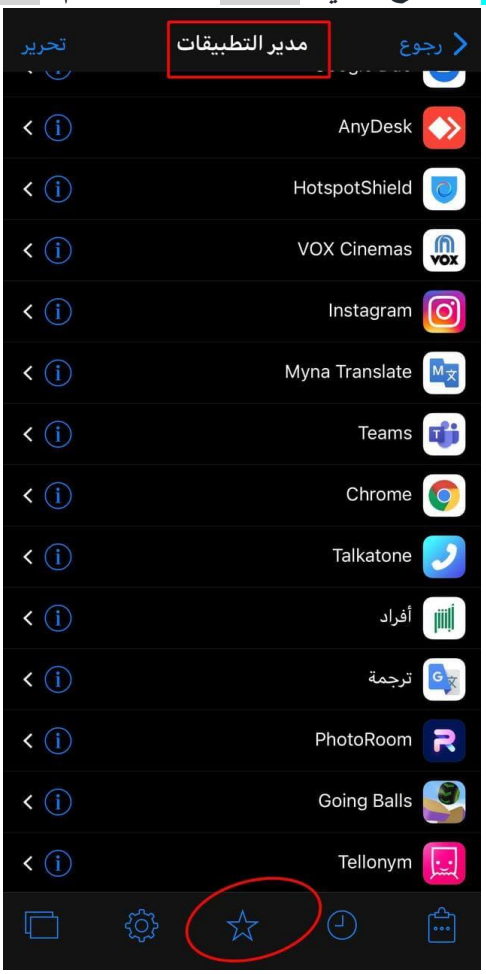
II7MAD99@GMAIL.COM 26 Oct 2021

كيف نستخرج معلومات تطبيق Twitter مثل الدايلب وغيرها؟
او واستخراج البيانات المخزنه في الايفون ؟

راح نستخدم الطريقة الاعتياديه من خلال أداة Fillza تستطيع تحميلها من السيديا - Cydia وتثبيتها

من خلال Fillza راح نستخرج بيانات التطبيقات واستعادة بعض الملفات وراح نستغل طرق كثيره مثل حفظ السنابات في سناب شات وغيرها

بعد تثبيت أداة Fillza نروح الي علامة النجمة ثم مدير التطبيقات



II7MAD99@GMAIL.COM 26 Oct 2021

الحين نبحث عن تطبيق Twitter ثم نضغط علامة التعجب

مثل ما تشاهد الصورة طلع لنا معرف التطبيق com.atebits.Tweetie2:

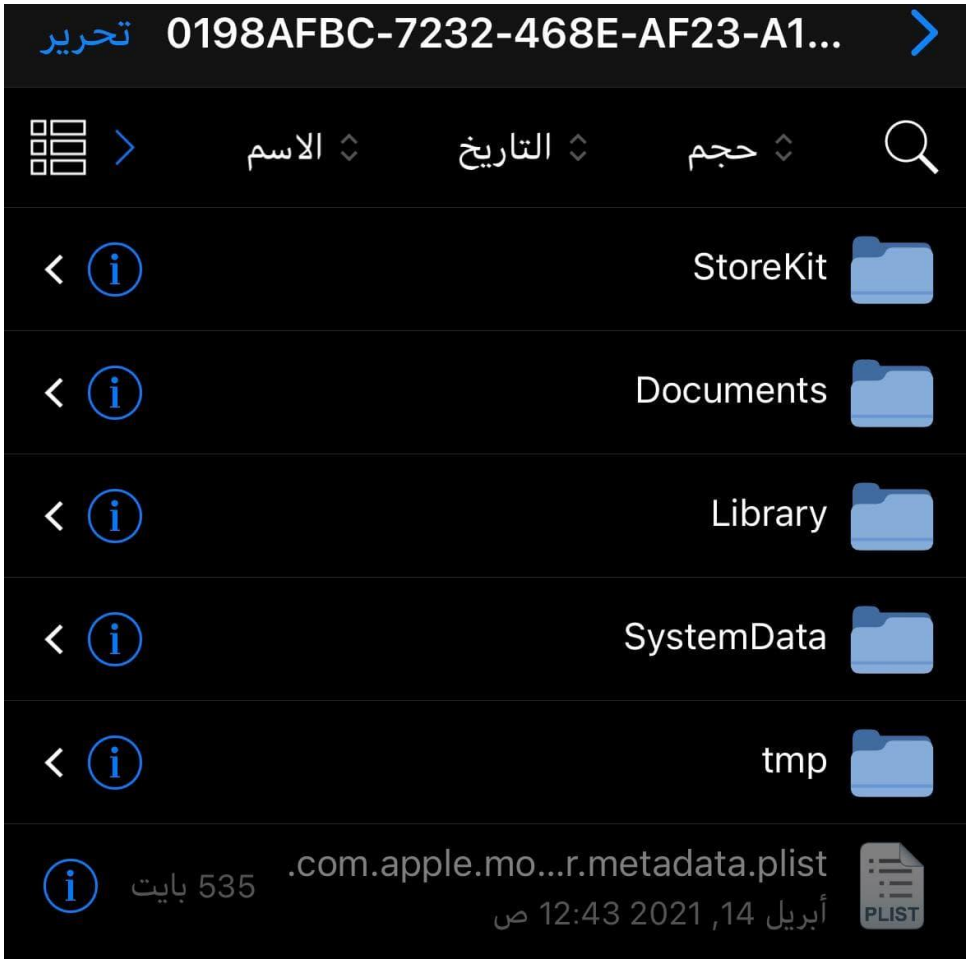
الإصدار : 8.60 والحزمة و البيانات

- الحزمة تعني ملفات التطبيق اللغة وصور العرض التويتر وغيرها
- البيانات تعني بيانات الحسابات التي تم ربطها في التطبيق مثل تسجيل الدخول وعدد الإضافات وغيرها حتى لو تم تسجيل خروج عن الحساب تبقي محفوظه

الان الي يهمنا فقط (البيانات) نضغط عليها

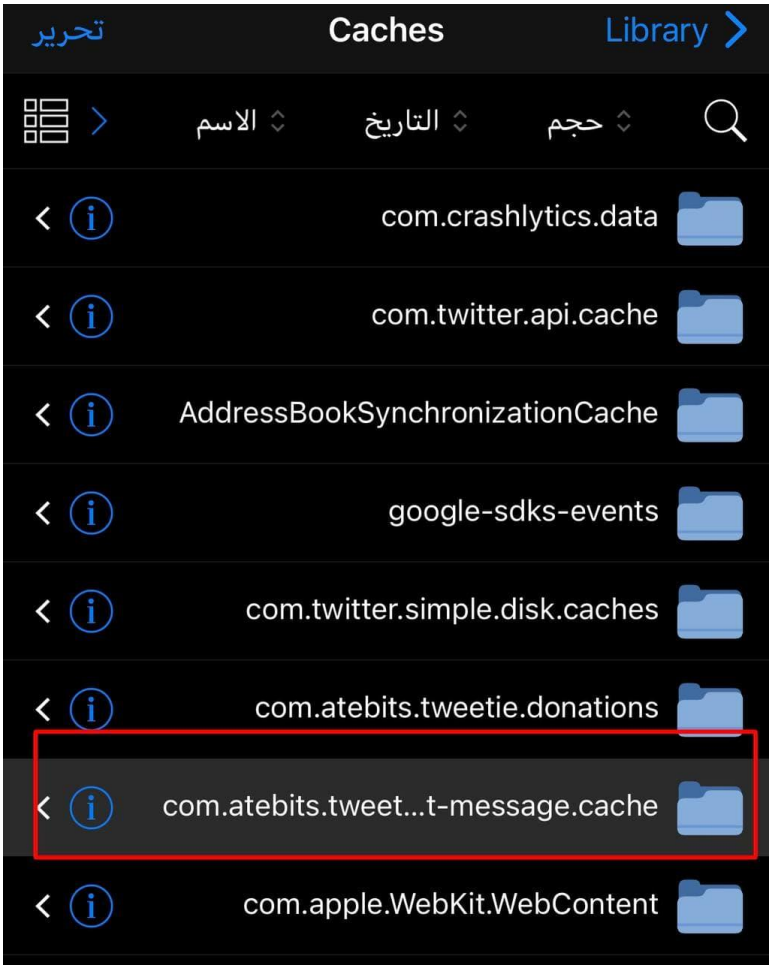
وراح تطلع لنا ملفات مثل الصورة التالية:

II7MAD99@GMAIL.COM 26 Oct 2021



الي يهمنا مجلدين فقط الي هم: Library وDocuments
راح نبدأ من مجلد Library ندخل عليه ثم مجلد Caches
ثم مجلد: com.atebits.tweetie.direct-message.cache

II7MAD99@GMAIL.COM 26 Oct 2021



عند الدخول على مجلد-com.atebits.tweetie.direct message.cache

راح تشوف الحسابات التي داخل عليها انت في تطبيق تويتر

II7MAD99@GMAIL.COM 26 Oct 2021

عند الضغط مثال على أحد الملفات الموجودة في المسار وضغط على objects راح يطلع لك الرسائل الخاص للحساب مع بعض البيانات في الخاص مثال:

يمكن ماتطلع لك كامله..

مطلوب تنزيلها من تطبيق ish :	Item 1604
Dictionary[22]	Item 1605
Dictionary[2]	Item 1606
Dictionary[2]	Item 1607
هاذي يافلاح مرتبة ؟	Item 1608
هاذي يافلاح مرتبة ؟	Item 1609
Dictionary[22]	Item 1610
Dictionary[2]	Item 1611
Dictionary[2]	Item 1612
لو ترسلها على الواتس بيكون افضل	Item 1613
لو ترسلها على الواتس بيكون افضل	Item 1614

طيب لو رجعنا للخلف الي مجلد Caches وندخل على مجلد :
com.atebits.tweetie.visited-links.cache

راح نشوف الحسابات الي سجلت دخول الي تطبيق تويتر حتى لو أحد الحسابات سجل خروج راح يتم حفظ اسم الحساب في هذا المسار

II7MAD99@GMAIL.COM 26 Oct 2021

في نفس المسار مجلد TIPImagePipeline راح تشوف الصور المخزنه من التويتر مثل صور التغريدات او صور الحسابات العرض وغيرها

طيب لو نطلع عن مجلد Library ونروح الي مجلد Documents
ندخل عليه ثم ندور علي مجلد :
com.atebits.tweetie.application-state

راح نشوف عمليات البحث الي صارت في الحسابات
مثل حساب test بحث عن هشتاق #أفضل_برمج

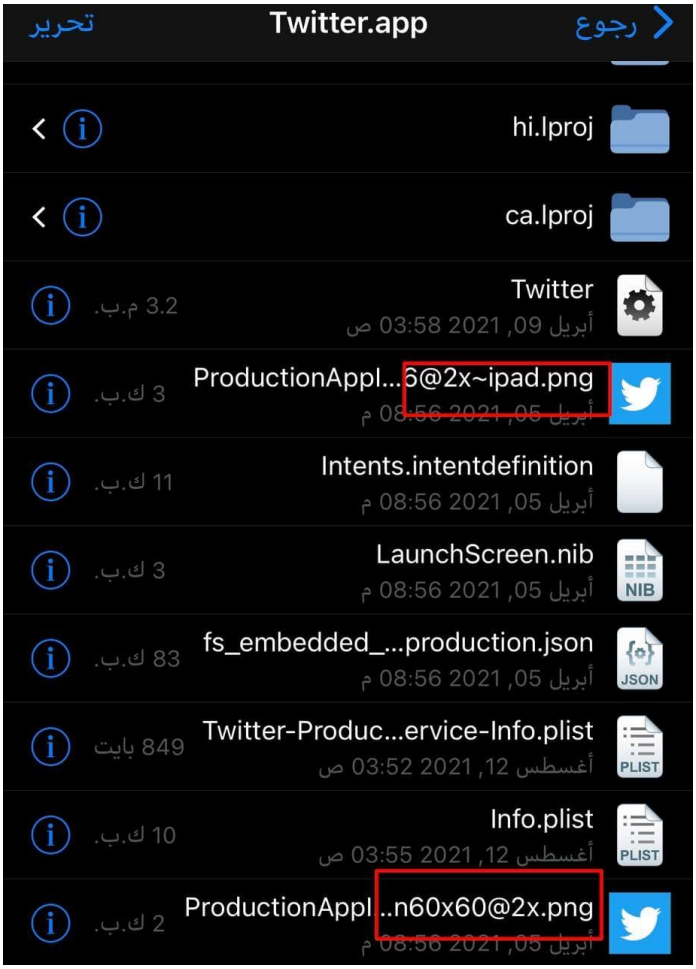
وغيرها ..

- بخصوص الحزمة التي تعني ملفات التطبيق اللغة وصور العرض التويتر تستطيع من خلالها تعديل على صور التطبيق مثل شعار تويتر

ملاحظه لازم يكون شعار الصورة متوافق مع حجم شعار تويتر وبنفس الاسم
مثال تنسخ اسم صوره شعار التويتر ونحذف الصورة الأصلية وتستبدل الاسم الي الصورة الجديدة تلاحظ بعدها تغير الشعار

حجم الصورة الاصلية للتويتر: 60x60
اسم الصورة: ProductionAppIcon60x60@2x.png

II7MAD99@GMAIL.COM 26 Oct 2021



اذا كان عندك جهاز ايباد تحتاج كذلك تحط الصورة بنفس حجمها والاسم الي مكتوب عليها ipad

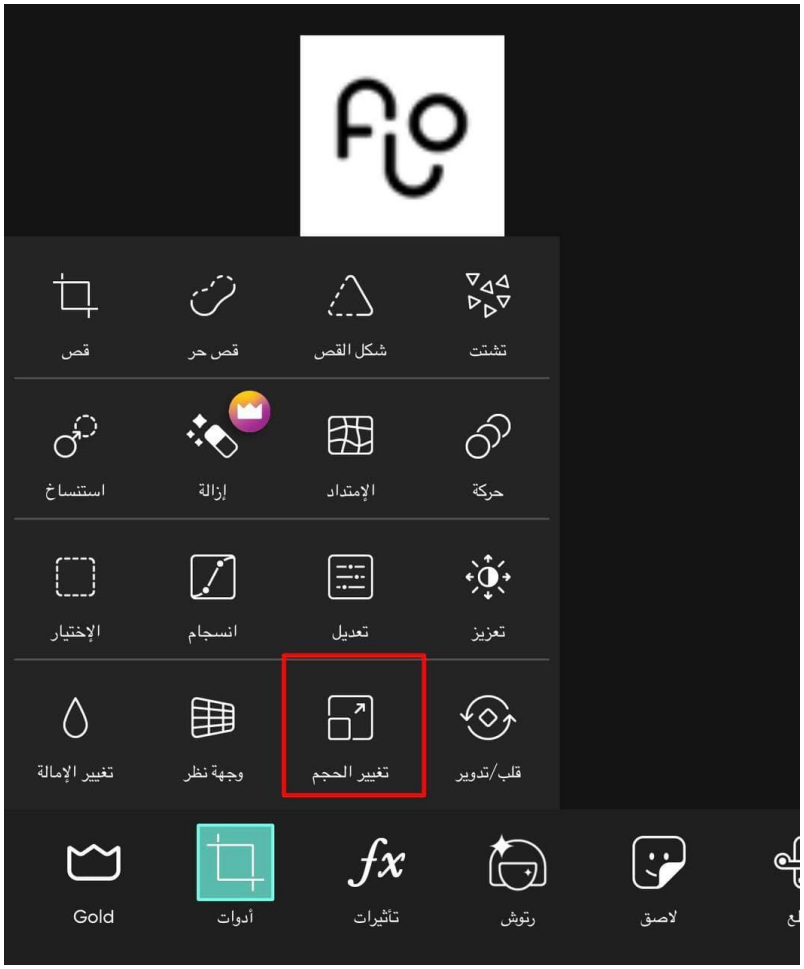
حجم الصورة الاصلية للتويتر: 76X76
اسم الصورة: ProductionAppIcon76x76@2x~ipad.png

كيف يتم تغير حجم الصورة الي حجم المطلوب؟

- **استخدم برنامج Picsart موجود في أبل ستور**

تابع الخطوات :

II7MAD99@GMAIL.COM 26 Oct 2021

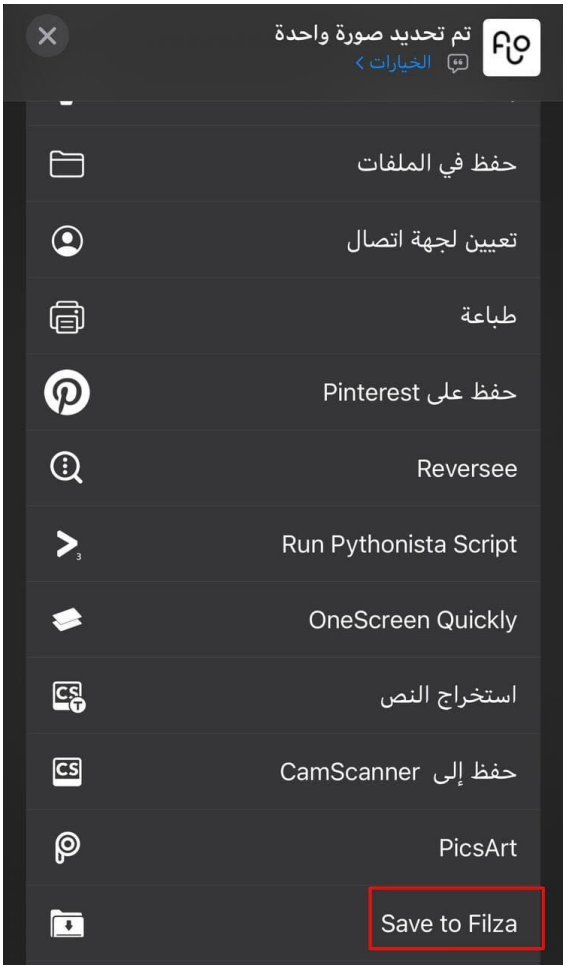


ثم نغير حجم الصورة الي الحجم المطلوب

II7MAD99@GMAIL.COM 26 Oct 2021

ثم نحفظ الصورة وندخل على الصور ثم مشاركه الي Fillza

II7MAD99@GMAIL.COM 26 Oct 2021



ثم نقل الصورة الي نفس المسار الموجود فيها الشعار ننسخ الاسم ونحذف الصورة الأصلية ونستبدلها في صورتنا

II7MAD99@GMAIL.COM 26 Oct 2021

كيذا استبدلنا صورة التطبيق بنجاح

للملاحظة عند اغلاق الجلبريك بعد التعديل على صورة التطبيق ما تقدر تدخل على التويتر لاحد ما تفعل الجلبريك - وجب التنبيه

تستطيع تبديل ملفات التطبيقات جميعها يعني مو بس على التويتر مثل تغير اسم التطبيق من ملف info.plist

في نفس مجلد Twitter.app بالإضافة التغيرات تنطبق على جميع التطبيقات مثل ما ذكرت في السابق بنفس الخطوات

II7MAD99@GMAIL.COM 26 Oct 2021

فحص تطبيق Tiktok

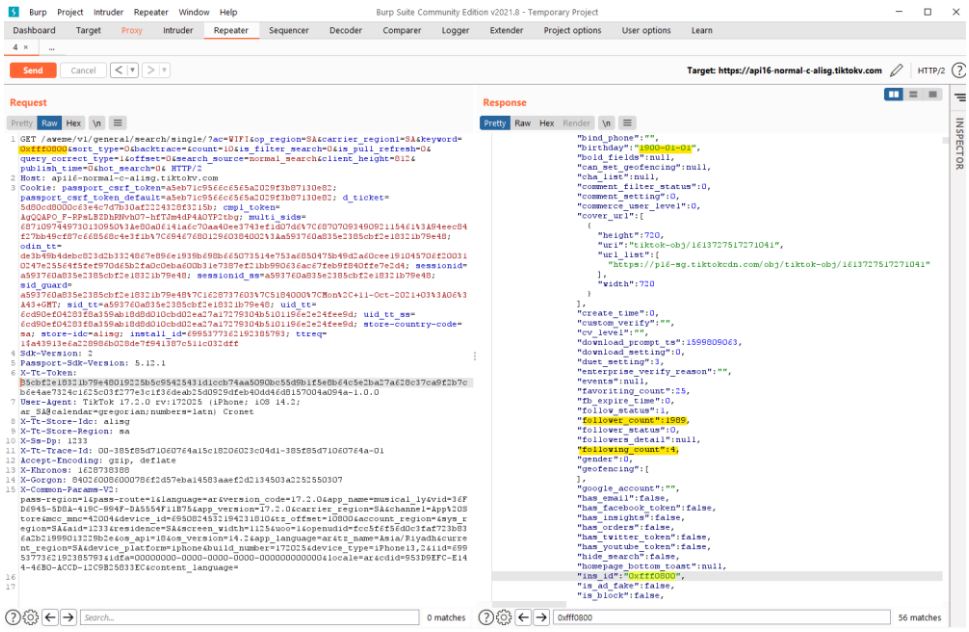
رجع اصدار تطبيق التيك توك الي ١٧,٢,٠

- نتأكد مفعلين خيار Intercept is on من Burp Suite
- نتأكد رابطين جوالنا في البرنامج Burp Suite
- نتأكد من اغلاق جميع التطبيقات من الخلفية ونجعل فقط تطبيق Tiktok

اول طلب البحث عن اسم المستخدم:

```
GET
/aweme/v1/general/search/single/?ac=WIFI&op_region=SA&carr
ier_region1=SA&keyword=0xfff0800&sort_type=0&backtrace=&co
unt=10&is_filter_search=0&is_pull_refresh=0&query_correct_
type=1&offset=0&search_source=normal_search&client_height=
812&publish_time=0&hot_search=0
```

تلاحظ استعلمت من داخل التطبيق عن اسم المستخدم `xfff0800 0`
خلينا نشوف البيانات الي طلعت لنا
نضغط كليك يمين في الماوس ونختار كلمة: Send to Repeater



II7MAD99@GMAIL.COM 26 Oct 2021

تلاحظ البيانات الي ظهرت غير موجودة في التطبيق مثل البلد SA وتاريخ الميلاد

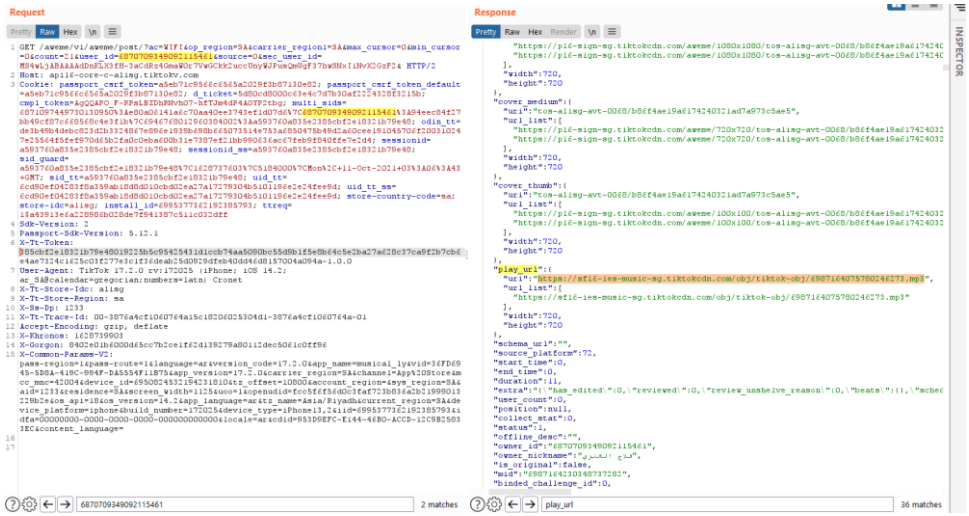
```
"birthday":"1900-01-01"
"follower_count":1989
"language":"ar"
"region":"SA"
"special_lock":1
```

وغيرها الكثير من البيانات..

طريقة استخراج الصوت والوصف والمقاطع وغيرها ندخل على الحساب من التطبيق ثم نشوف الطلب في برنامج: Burp

```
GET
/aweme/v1/aweme/post/?ac=WIFI&op_region=SA&carrier_region1
=SA&max_cursor=0&min_cursor=0&count=21&user_id=68707093490
92115461&source=0&sec_user_id=MS4wLjABAAAAdDnKLX3fH-
3aCdRz4GmaW0r7VwGCkk2uccUnyWJPusQmUgF37hwSNxIiNvX2GzF2&
```

تلاحظ مكتوب امامك في الطلب user_id وهو معرف الحساب الي استعلمنا عنه طيب يوم ضغطت send رد السيرفر وجاب لي البيانات التاليه



تلاحظ جاب لي:

https://sf16-ies-music-sg.tiktokcdn.com/obj/tiktok-obj/6987164075780246273.mp3

وهذا الرابط الصوت الفيديو طيب كيف اسحب المقطع كامل مع الصوت؟

II7MAD99@GMAIL.COM 26 Oct 2021

ابحث لي عن كلمة play_addr في رد السيرفر

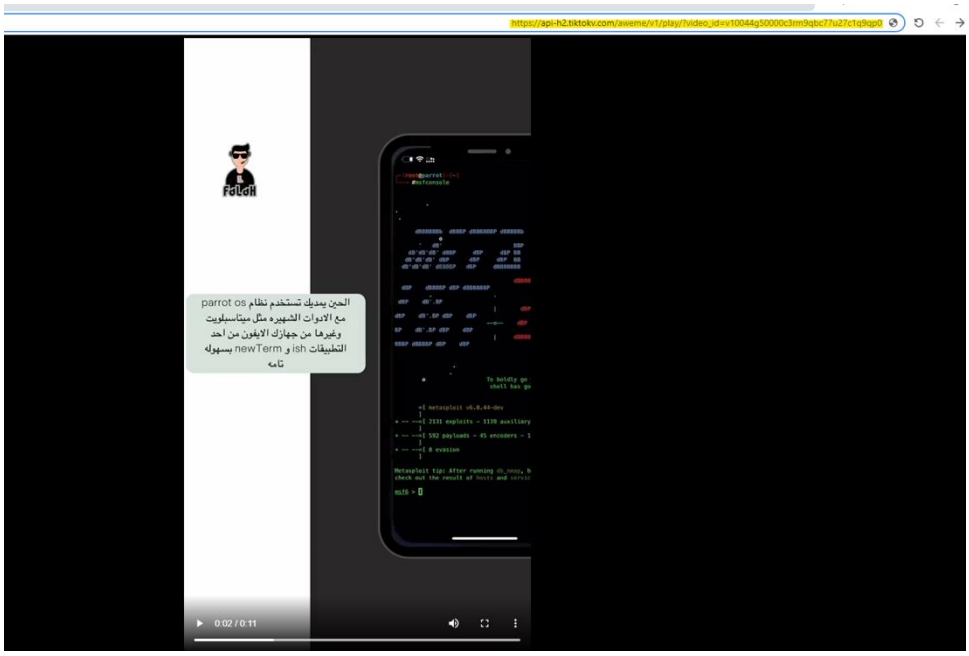

```
"play_addr_265":{
  "uri":"v10044g50000c3rm9qbc77u27c1q9qp0",
  "url_list":[
    "https://v77.tiktokcdn.com/87eac9688318feac899294b83ec0ff94/6114ee13/video/tos/alisg/tos-alisg-pve-0037c00
    D\u0026vl=\u0026vr=",
    "https://v16m.tiktokcdn.com/54426cb4751551ca2d9c9432eeb6830e/6114ee13/video/tos/alisg/tos-alisg-pve-0037c0
    3D\u0026vl=\u0026vr=",
    "https://api-h2.tiktokv.com/aweme/v1/play/?video_id=v10044g50000c3rm9qbc77u27c1q9qp0\u0026line=0\u0026is_p
  ],
  "width":720,
  "height":720,
  "url_key":"v10044g50000c3rm9qbc77u27c1q9qp0_bytevc1_540p_271865",
  "data_size":378674,
  "file_hash":"444c23f8703f3bdd8d66311016fa4640",
  "file_cs":"c:0-10524-4052"
},
"is_h265":1,
"play_addr_h264":{
  "uri":"v10044g50000c3rm9qbc77u27c1q9qp0",
  "url_list":[
    "https://v77.tiktokcdn.com/ff45e15374773f55dfa93b772cb83534/6114ee13/video/tos/alisg/tos-alisg-pve-0037c00
    D\u0026vl=\u0026vr=",
    "https://v16m.tiktokcdn.com/c9aae48c38a182ec848605dd2d3874de/6114ee13/video/tos/alisg/tos-alisg-pve-0037c0
    https://api-h2.tiktokv.com/aweme/v1/play/?video_id=v10044g50000c3rm9qbc77u27c1q9qp0 u0026line=0\u0026is_p
```


بيطلع عندك رابط المقطع لا تنسخه كامل فقط انسخ من
https://api-h2.tiktokv.com
الي
video_id=v10044g50000c3rm9qbc77u27c1q9qp0

يعني يكون الرابط في أشكل هذا:

https://api-h2.tiktokv.com/aweme/v1/play/?video_id=v10044g50000c3rm9qbc77u27c1q9qp0

الصق الرابط في المتصفح راح يطلع لك الفيديو كامل وتستطيع حفظه:



II7MAD99@GMAIL.COM 26 Oct 2021

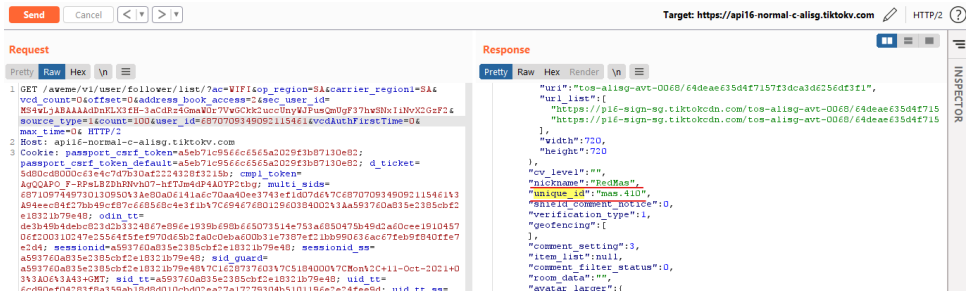
طلب جلب متابعين الحساب:

تدخل على الحساب المراد جلب متابعينه ثم تضغط علي المتابعون راح يطلع عندك في الطلب

```
GET
/aweme/v1/user/follower/list/?ac=WIFI&op_region=SA&carrier
_region1=SA&vcd_count=0&offset=0&address_book_access=2&sec
_user_id=MS4wLjABAAAAdDnKLX3fH-
3aCdRz4GmaW0r7VwGCkk2uccUnyWJPusQmUgF37hwSNxIiNvX2GzF2&sou
rce_type=1&count=100&user_id=6870709349092115461&vcdAuthFi
rstTime=0&max_time=0& HTTP/2
```

= count=100 جب لي 100 حساب يتابعه

اذا عدلت على follower بنفس الطلب الي following راح تجيب حسابات الي يتابعهم صاحب الحساب



ابحث عن unique_id ويعني اسم المستخدم بخصوص nickname ويعني النك نيم

```
"nickname":"RedMas","unique_id":"mas.410"
```

حتى تقدر تعرف عدد الي يتابعونهم من following_count لكل حساب

مثال:

II7MAD99@GMAIL.COM 26 Oct 2021

"following_count":420,"show_image_bubble":
false,"language":"en","unique_id":"mk4_w"

اسم المستخدم : mk4_w يتابع 420 حساب

وإذا تبي تعرف id الحسابات تبحث عن كلمة : uid
"uid":"6981606380927828994

معرفة بلدان الحسابات من عند: region

"region":"SA"

طيب كيف يتم زيادة المشاهدات المقاطع؟

بخطوات سهله تروح تضغط على الفيديو الي ترغب برفع مشاهداته
راح يطلع عندك في الطلب:

POST
/aweme/v1/aweme/stats/?ac=WIFI&op_region=SA&carrier_region
1=SA&

Host: api16-core-c-alisg.tiktokv.com

II7MAD99@GMAIL.COM 26 Oct 2021


```
1  POST /aweme/v1/aweme/stats/?ac=WIFI&op_region=SA&carrier_region1=SA& HTTP/2
2  Host: api16-core-c-alisg.tiktokv.com
3  Cookie: passport_csrf_token=a5eb71c9566c6565a2029f3b87130e82; passport_csrf_token_default=
   a5eb71c9566c6565a2029f3b87130e82; d_ticket=5d80cd8000c63e4c7d7b30af2224328f3215b; cmpl_token=
   AgQQAPO_F-RPsLBZDhRNvh07-hfTJm4dP4AOYP2tbg; multi_sids=
   6871097449730130950%3Ae80a06141a6c70aa40ee3743ef1d07d6%7C6870709349092115461%3A94eec84f27bb49cf87c668568c4e3f1b%7
   C6946768012960384002%3Aa593760a835e2385cbf2e18321b79e48; odin_tt=
   de3b49b4debc823d2b3324867e896e1939b698b665073514e753a6850475b49d2a60cee19104570bf200310247e25564f5fef970d65b2fa0c
   0eba600b31e7387ef21bb990636ac67feb9f840ffe7e2d4; sessionid=a593760a835e2385cbf2e18321b79e48; sessionid_ss=
   a593760a835e2385cbf2e18321b79e48; sid_guard=
   a593760a835e2385cbf2e18321b79e48%7C1628737603%7C5184000%7CMon%2C+11-Oct-2021+03%3A06%3A43+GMT; sid_tt=
   a593760a835e2385cbf2e18321b79e48; uid_tt=6cd90ef04283f8a359ab18d8d010cbd02ea27a17279304b5101196e2e24fee9d;
   uid_tt_ss=6cd90ef04283f8a359ab18d8d010cbd02ea27a17279304b5101196e2e24fee9d; store-country-code=sa; store-idc=
   alisg; install_id=6995377362192385793; ttreq=1$a43913e6a228986b028de7f941387c511c032dff
4  Content-Length: 117
5  Sdk-Version: 2
6  Passport-Sdk-Version: 5.12.1
7  X-Tt-Token:
   01a593760a835e2385cbf2e18321b79e48019225b5c95425431d1ccb74aa5090bc55d9b1f5e8b64c5e2ba27a628c37ca9f2b7cb6e4ae7324c
   1625c03f277e3c1f36deab25d0929dfeb40dd46d8157004a094a-1.0.0
8  Content-Type: application/x-www-form-urlencoded
9  User-Agent: TikTok 17.2.0 rv:172025 (iPhone; iOS 14.2; ar_SA@calendar=gregorian;numbers=latn) Cronet
10 X-Ss-Stub: 23E7AF6D29AAFD4F36C8DAE09A6F9D9F
11 X-Tt-Store-Idc: alisg
12 X-Tt-Store-Region: sa
13 X-Ss-Dp: 1233
14 X-Tt-Trace-Id: 00-38d1a8451060764a15c18206024204d1-38d1a8451060764a-01
15 Accept-Encoding: gzip, deflate
16 X-Khronos: 1628745868
17 X-Gorgon: 8402006160000ecac01f8f7cda4974632ccbffbe64e51dc220a35
18 X-Common-Params-V2:
   pass-region=1&pass-route=1&language=ar&version_code=17.2.0&app_name=musical_ly&vid=36FD6945-5D8A-419C-994F-DA5554
   F11B75&app_version=17.2.0&carrier_region=SA&channel=App%20Store&mcc_mnc=42004&device_id=6950824532194231810&tz_of
   fset=10800&account_region=&sys_region=SA&aid=1233&residence=SA&screen_width=1125&uoo=1&openudid=fcc5f6f56d0c3faf7
   23b836a2b21999013229b2e&os_api=18&os_version=14.2&app_language=ar&tz_name=Asia/Riyadh&current_region=SA&device_pl
   atform=iphone&build_number=172025&device_type=iPhone13,2&iid=6995377362192385793&idfa=00000000-0000-0000-0000-000
   000000000&locale=ar&cdid=953D9EFC-E144-4EB0-ACCD-12C9B25833EC&content_language=
19
20 action_time=1628745870&aweme_type=0&first_install_time=1618365239&item_id=6987164275160681730&play_delta=1&
   tab_type=4
```

مثل ما تلاحظ الداتا هي:

action_time=1628745870&aweme_type=0&first_install_time=1618365239&item_id=6987164275160681730&play_delta=1&tab_type=4

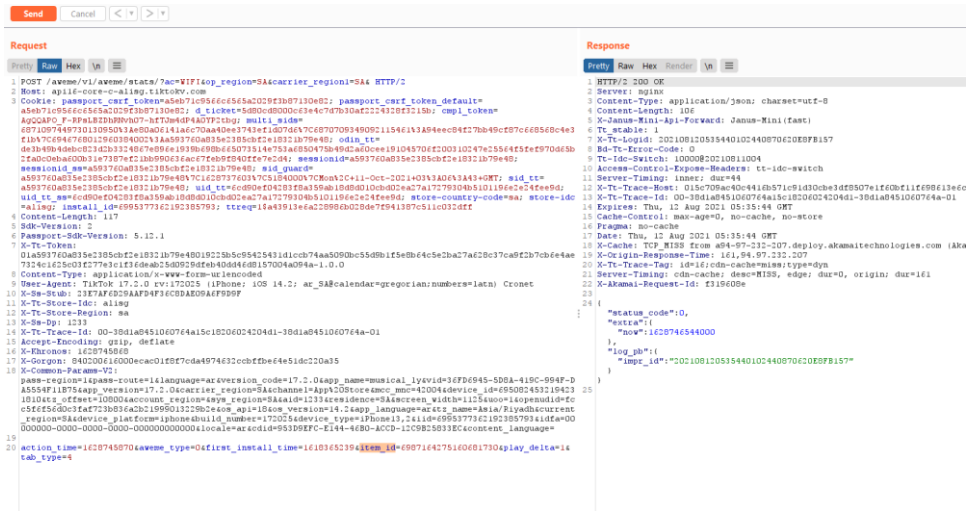
ويعني action_time الوقت بلغة الكمبيوتر
ويعني item_id معرف المقطع الي دخلت عليه

قبل ما نزيد مشاهدات المقطع اول شيء نشوف كم عدد المشاهدات

كويس عدد المشاهدات هي 3874 الحين راح نرفعها للعدد الي نبيه
كيف؟ نروح عند الطلب ونضغط send مره وحده راح يصير العدد 3875

وكل ما رجعت وضغطنا send بنفس الطلب راح نرفع المشاهدات

II7MAD99@GMAIL.COM 26 Oct 2021



الرد يكون:

{"status_code":0,"extra":{"now":1628746544000},"log_pb":{"impr_id":"20210812053544010244087062 0E8FB157"}}

لكن لو طلع لك:

{"status_code":5,"status_msg":"معلمات غير صالحة"}

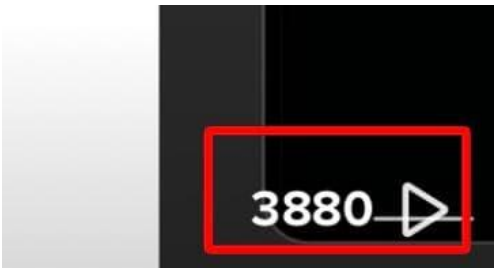
فيه خطاء في الطلب وغالبا يكون من معرف المقطع او الوقت

اذا طلع لك :

{"log_pb":{"impr_id":"20210812053920010244082047038EC58F"},"status_code":0,"extra":{"now":1628746760000}}

يعني طلبات متكررة بسرعه عالية وللأسف ماراح يحسب رفع المشاهدة

كررت الطريقة بنسبه لي 5 مرات والنتيجة:



مثل ما تشوف تم رفع المشاهدات

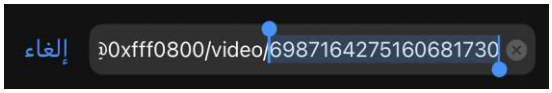
II7MAD99@GMAIL.COM 26 Oct 2021

اذا برمجة أداة بلغة البايثون بنفس الطلب حق رفع المشاهدات راح تكون النتيجة حلوة جدا لكن لا تنسي تعمل بين كل 5 رفع مشاهدات sleep لا مدة 10 ثواني

اذا غيرت item_id و حطيت معرف مقطع ثاني راح ترفع مشاهداته بنفس الطلب

```
action_time=1628745870&aweme_type=0&first_install_time=1618365239&item_id=6987164275160681730&play_delta=1&tab_type=4
```

وغالبا معرف الفيديوهات يكون في رابط مشاركة الفيديو تنسخه وتحطه في الويب وتضغط انتر وراح يطلع معرف الفيديو مثال:



فحص تطبيق Snapchat

رجع اصدار تطبيق سناب شات الي ١٠,٨٢,٠,٧٣

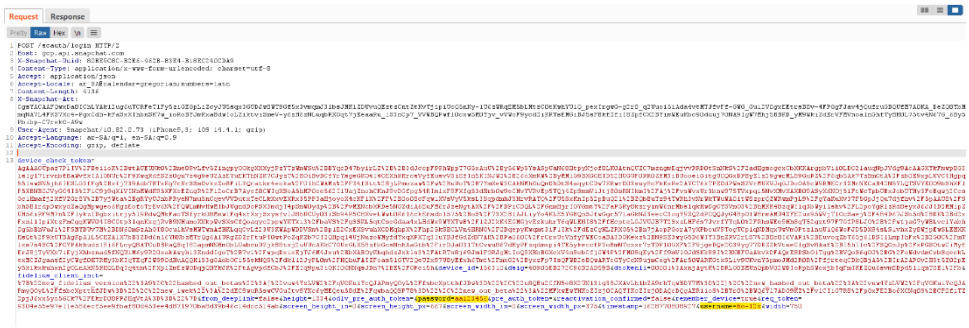
- نتأكد مفعلين خيار Intercept is on منBurp Suite
- سجل خروج عن الحساب المرتبط في السناب
- نتأكد رابطين جوالنا في البرنامجBurp Suite
- نتأكد من اغلاق جميع التطبيقات من الخلفية ونجعل فقط تطبيق Snapchat

التسجيل الدخول في السناب:

```
POST /scauth/login HTTP/2
Host: gcp.api.snapchat.com
X-Snapchat-Uuid: 80BE9C8C-B2E6-462B-B3E4-B18EC240CDA9
Content-Type: application/x-www-form-urlencoded; charset=utf-8
```

II7MAD99@GMAIL.COM 26 Oct 2021


```
Accept: application/json
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 4136
X-Snapchat-Att:
CgsYACAAFQwxDa8IChLYAk12ug6uTCRFeTlFy5ziGEGpLiZcyJU5sqx3GUDJw8WT9Gf5
x3vmqmJ3lbsJMK1ZDUvuQEztzCntZtKvTjipiUcQ5nKy-
1U6zWRqEM5bLMtzC0tKwhYU1Q_pexIrgwG-g2r8_q2Uuoi5iAda4vtMTJfvFf-
GWG_Gu12V0gxEEtrsB8v-
4FPGgFJav4jQufruGBQUfM7A0KA_DeZQ8YbMmqNA7L4FKS7Xc4-PgxCdh-
kFaSxXIhbnSK7w_ioRoBYJmKxaBdwIoLZiktviSmeV-
y6zH6zNLuqbRXOqt7jEeaaRu_lS3nCp7_VVWBQPwfl0cxw5M0Yjv_vVWoF9ycd2iKRTs
EMGiBJ5sFBkf2fiI8ZpfCX2BYimWEuKbc90duuj70NA9lgW7Mhj5BBKD_yM9WkiZdErV
FMVnoalnGhfTyHH0L75tv4N67G_6By5Pbibp-C7rekO-A9w
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate
```

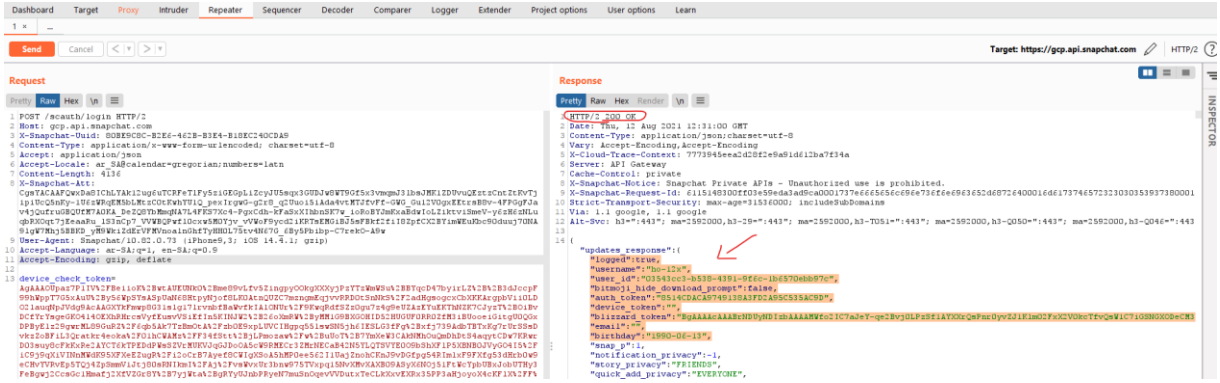


تلاحظ في الداتا password و: username

طلعت عندي في الطلب لأني حطيت اسم المستخدم
في التطبيق ho-12x: وكلمة المرور الحساب:aa123456

لو حبينا نضغط send ونشوف رد السيرفر

II7MAD99@GMAIL.COM 26 Oct 2021



تم تسجيل دخول بنجاح للحساب:

"logged":true,"username":"ho-12x","user_id":"03543cc3-b538-4391-9f6c-1b6570ebb97c","bitmoji_hide_download_prompt":false,"auth_token":"8514CDACA9749138A3FD2A95C535AC9D","device_token":"","blizzard_token":"BgAAAAcAAABrNDUyNDIzbAAAAMWfo2IC7aJeY-qe2Bvj0LPzSf1AYXXrQsPnr0yvZJ1Klm02FxX2V0kcTfvQsW1C7iGSNGXODeCM3tu9x3e8bd05ytyALyIOB_I1Cr_KP7tfCG0GzD8bsNq4Gm2M5lOsBFhK0sU9U7r-bDhQ0A4AAABibGl6emFyZC10b2tlbhAAAADny7fuHSo7e__h0xGXOpNO","email":"","birthday":"1990-06-13

لو كانت كلمة المرور خطاء بيكون الرد:

"{"logged":false,"message":"عفوًا، لا يمكننا العثور على بيانات اعتماد مطابقة.","status":-100,"display_register_cta":false}"

لو كان فيه تعديل في بيانات الطلب راح يكون الرد :

"{"logged":false,"message":"عفوًا! أنت تحاول الوصول إلى Snapchat بواسطة تطبيق خاص بجهة خارجية! يُرجى استخدام تطبيق Snapchat الرسمي بدلاً من ذلك لو سمحت . 😉"}

لو طلع لك في رد السيرفر :

انت تستخدم اصدار Snapchat ونظام تشغيل لم يعد مدعوما

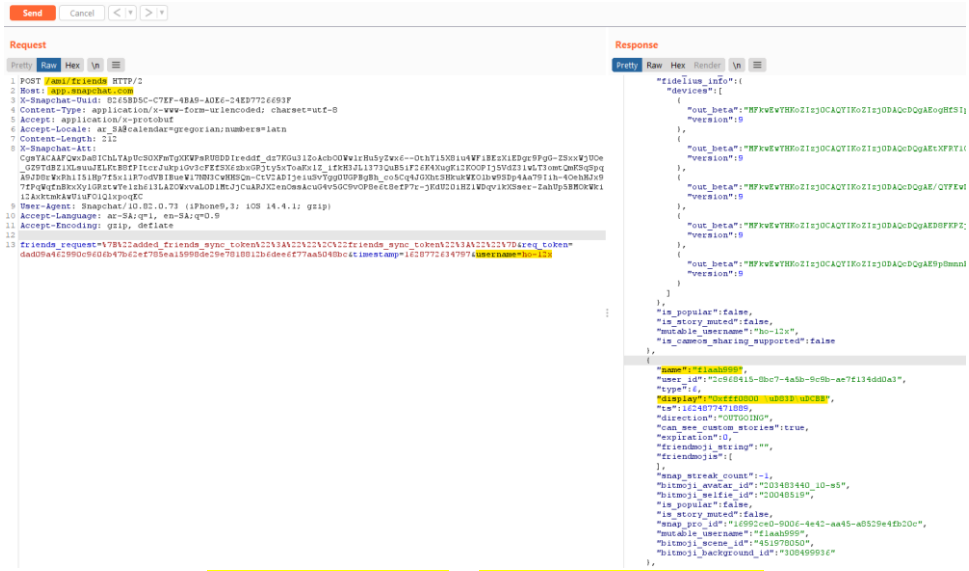
حاول تحدث التطبيق الي اصدار أحدث من ١٠,٨٢,٠,٧٣ بتحديث الي بعده مثال: ١٠,٨٢,٥,٧٥

II7MAD99@GMAIL.COM 26 Oct 2021

الي اتابعهم ويتابعوني في الطلب:

```
POST /ami/friends HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: 8265BD5C-C7EF-4BA9-A0E6-24ED7726693F
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/x-protobuf
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 212
X-Snapchat-Att: CgsYACAAFQwxDa8IChLYApUcS0XFmTgXKWPsRU8DDIreddf_dz7KGu3lZoAcbO0WwlrHu5yZwx6--
0thY15X8iu4WFiBEzXiEDgr9PgG-
ZSxxWjUOe_GZ9TdBZ1XLsuuJELKtB8fPItcrJukpiGv3cFEfSX6zbxGRjty5xToaKxlZ_ifkH3JLl373QuB5iF26K4XugKi2KOOPIj5Vd
Z31wLT3omtQmKSqSpqA9JD8rWxRh1I51Hp7f5xl1R7odVBIBueW17NN3CwHHSQn-
CtV2ADIjeiuSvYgg0UGPBgBh_co5Cq4JGXhtSHkukWEOlbw9SDp4Aa79Iih-
4OehHJx97fPqWqfnBkxXylGRztwYelzh613LAZOWxvaL0DlMtJjCuARJX2enOssAcuG4v5GC9vOP8e6t8efP7r-
jKdU20iHZ1WDqv1kXSser-ZahUp5BMOkWkii2AxktmkAwUiuFO1QlxpoqEC
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

friends_request=%7B%22added_friends_sync_token%22%3A%22%22%2C%22friends_sync_token%22%3A%22%22%7D
&req_token=dad09a462990c9606b47b62ef785ea15998de29e7818812b6dee6f77aa5048bc&timestamp=1628772634797
&username=ho-12x
```

رد السيرفر:



name":"flaah999" , "display":"0xfff0800"

Name : اسم الحساب الي اتابعه

Display : نك نيم الحساب

II7MAD99@GMAIL.COM 26 Oct 2021

طلب أقترح الأصدقاء:

```
POST /bq/suggest_friend HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: 5AF272D6-0655-4470-AFF5-4253E74750E6
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 126
X-Snapchat-Att:
CgsYACAAFQwxDa8IChLcAsDXiLv3htlZliUj2Mvs0Qvnv30Rlaiag_cwgxRnr1POgSQz92PEQs01SJ1YAc
QwYZ-3anw2nUoLHcywVBKq89yIHL6h3mrMAzADgwHT_5isk3eYs_3HR31ZTCWr6-
17PZdNAM7MizLowuhgt-
YS5CdisJq8Rv6AVWywOA5Ywo_Bxooxk8YpSkI2m2nAhqKjXj_h5nBA7YZFYyxCOnO_Aaa5aX7Oo4ZP
S8kFbb5gzgdepbRcpbQYpTC_Zr2j2QOZU7ssxrPX1OCyD_7BjQbB1j_TnkFbuDuIa6TgiUzz3Z7YGDy1H
_a6E7XMcyQ2DZ4aRC09hNx7v9pzPDeI35jGSyOsgH0DsiSAo0RK-UOr9c3oYe1RzUw70Bc6pVQK-
2BCBuXFwc0yuWRPopgTT8kxGuqo2zXvUg9VeRmO6idoG4A1hh4uw7xTNbyY5rKSytVIh8ipL8EphIct
qZ7lCQ==
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

action=list&req_token=dade254186109a306bc0462eff89b4f5618be2937860b1233dee6577ad5043
fc&timestamp=1628772634800&username=ho-12x
```

قراءة محادثات الخاص من حسابك من خلال الطلب:

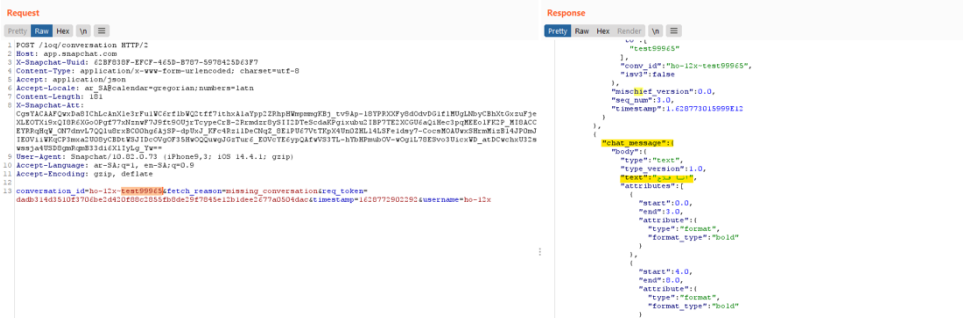
```
POST /loq/conversation HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: 62BF838F-EFCF-465D-B787-5978425D63F7
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 181
X-Snapchat-Att:
CgsYACAAFQwxDa8IChLcAnXle3rFu1WC6rflbWQ2tff7ithxAlaYpp2ZRhpHWmpmmgKBj_tv9Ap-
l8YPRXXFy8dOdvDG1flMUgLNbyCBhXtGxzuFjeXLEOTXi9xQI8R6XGoOPgf77xNznwF7J9ft9OUjrTcyp
eCrB-
2Rrmdzr8ySII2DTeScdaKPgixubu2IBP7TE2XCGU6aQiHec3pqMEEolFK2P_MI8ACCEYRRqHqW_ON7d
nvL7QQlu8rxBC00hg6AjSP-dpUxJ_KFc4Rz1lDeCNqZ_8E1PU67VtTKpX4Un0ZHLl4LSFe1dsy7-
CocsMOAUwxSHrmMizB14JP0mJIE0ViiWKqCP3mxa2U08yCBDtWSJIDcOVgOF35HwOQQuwgJGzTur
6_E0VcYE6ypQAfwVS3TL-hYbHPmubOV-
wOg1L78ESvo3UicxWD_atDCwchxU32swssja4USD8gmRqmB33di6XllyLg_Yw==
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
```

II7MAD99@GMAIL.COM 26 Oct 2021

Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

conversation_id=ho-12x~test99965&fetch_reason=missing_conversation&req_token=dadb314d3510f3706be2d420f88c2855fb8de29f7845e12b1dee2677a0504dac&timestamp=1628772902292&username=ho-12x

طلبت اقراء محادثه conversation_id=ho-12x~test99965
وهو عندي متابع أقدر استعلم عن حساب ثاني بمجرد ماغير من ho-12x~test99965 الي ho-12x~flaah999



تلاحظ كلمة text وتعني الرسالة الي مكتوبه في المحادثة بين الطرفين

كيف اعرف وقت الرسالة ؟ من عند last_read_timestamp وهي موجودة في اخر رد السيرفر مثل:
"last_read_timestamp":1628773066263

معني last_read_timestamp آخر طابع زمني للقراءة
وتعني last_write_timestamp آخر طابع زمني للكتابة

طيب عشان تعرف الوقت بساعات وتاريخ تنسخ الرقم الموجود عندك في last_read_timestamp مثال عندي:
١٦٢٨٧٧٣٠٦٦٢٦٣

نروح الي موقع www.epochconverter.com :

وتلصق الي نسخته ١٦٢٨٧٧٣٠٦٦٢٦٣ راح يطلع لك الوقت وتاريخ

II7MAD99@GMAIL.COM 26 Oct 2021

Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1628775479

Convert epoch to human-readable date and vice versa

1628773066263 | Timestamp to Human date | [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **milliseconds**:

GMT : Thursday, August 12, 2021 12:57:46.263 PM
Your time zone : Thursday, August 12, 2021 3:57:46.263 PM GMT+03:00
Relative : 2 minutes ago

Yr	Mon	Day	Hr	Min	Sec	
2021	8	12	12	58	54	GMT

Human date to Timestamp

طلع عندي وقت كتابه المحادثة الساعة ٣:٥٧ م

للمعلوميه اذا صاحب الحساب رد عليك ورسل لك رسالة واستعلمت بنفس الطلب الي فوق
ماراح يطلع عنده أنك قريت المحادثة

طلب فك الحظر عن حساب محدد :

```
POST /bq/friend HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: 66FC74C9-1C7E-45E6-85C5-086CC814BB3C
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/x-protobuf
```

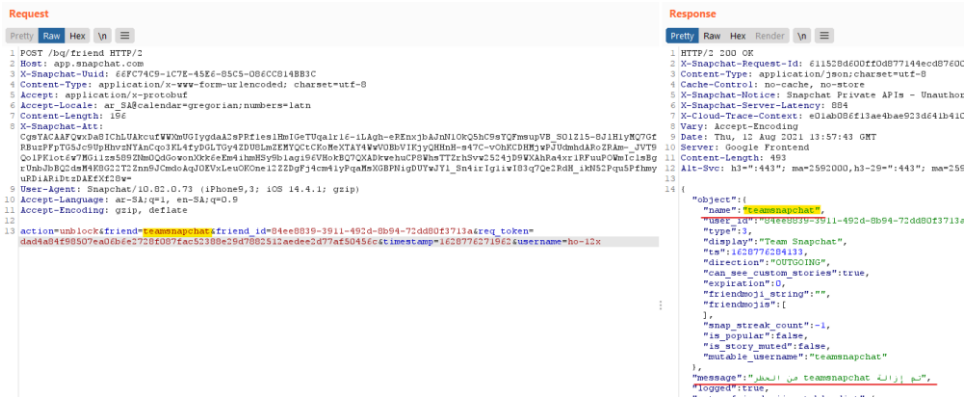
II7MAD99@GMAIL.COM 26 Oct 2021

Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 196
X-Snapchat-Att: CgsYACAAFQwxDa8IChLUAkcufWWXmUGIygdaA2sPRf1eslHmIGeTUqalr16-iLAgh-eRExjbAJnN1OkQ5hC9sYQFmsupVB_S0lZl5-8JlH1yMQ7GfRBuzPFpTG5Jc9UpHhvzNYAnCqo3KL4fyDGLTGy4ZDU8LmZEMYQCtCKoMeXTAY4WwV0BbVIKjyQHHnH-s47C-vOhKCDHMjwPJUdmhdARoZRAm-_JVT9QolPK1ot6w7MGi1zs589ZNm0QdGowonXkk6eEm4ihmHSy9b1agi96VHokBQ7QXADkwehuCP8WhsTTZrhSvw2524jD9WXAhRa4xr1RFuuPOWmIclsBgrUnbJbBQ2dsM4K8G22T2Znn9JCmdoAqJ0EVxLeuOKOne12ZZDgFj4cm41yPqaMsXGBPNigDUYwJYl_Sn4irIg1iwI83q7Qe2RdH_ikN52Pqu5PfhmyuRDiARi
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

action=unblock&friend=teamsnapchat&friend_id=84ee8839-3911-492d-8b94-72dd80f3713a&req_token=dad4a84f98507ea06b6e2728f087fac52388e29d7882512aedee2d77af50456c&timestamp=1628776271962&username=ho-12x

- **تشوف كلمة friend وتعني فك الحظر عن حساب teamsnapchat**

نشوف رد السيرفر:



"message":"تم إزالة teamsnapchat من الحظر

طلب حظرحساب محدد:

POST /reporting/inapp/v1/user HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: B124C279-B265-4185-8FBE-0260962275A6
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: */*

II7MAD99@GMAIL.COM 26 Oct 2021

Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 218
X-Snapchat-Att:
CgsYACAAFQwxDa8IChLkAkFdiW8p8NnopVu8IwLhPbu0IJB3Cug2uOaBcNOVJliDFExw-mL1dVImG8Yq2NjNfgvL7KTY7rYKDK7M3_piWg7b7BMxe8iP-0BcSBSdynM_iei0ngYMwEbwlPziyl_qyIphf6Q_imzoB2xsImzU_FQbBEBQxOctmIrL2tfmB0DivXm4Qa9_ZqpuFt8Yq4WsrZ6B4KDKD5r5I4BFN7HzGG-skULN2zIs8dMVF0zg08dk77M0MPCxkkbJQbtD2dmzp3VV2j2jgtrDIrd64UgX4yRQsjz2h5vQXWCgO731pqJzxGA78X_UhIEAxnlXJdjWyMM_4ZFi_ViasEaZf2phaOVeiFQMhg7at3r5-_Csd_XahGRNdsvONMAKnfIYLlQu2FEgnEe6s7OwYeNCzgt6lFph2_ug1MK8lo7tMkErVlSohl4NnFAaAak_nYcROzauTUVIE258lr8AFRRdEfQtY9Rn7wxk
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

context=&friend_link_type=0&reason_id=report_user_reason_mean_or_inappropriate_snaps&reported=test99965&req_token=dad4214427307b606bb0a720f2822d15ba82e29b789e9122adee6477ae504d3c&timestamp=1628777234994&username=ho-12x

تلاحظ طلب اني اسوي بلاغ على حساب test99912
نشوف رد السيرفر

الرد HTTP/2 200 OK يعني تم ارسال البلاغ بنجاح لو سويت لك أداة في البايثون النتيجة تكون ممتازة في محاسبة الحسابات الإباحية واغلاقها للأبد

طلب الحسابات عن حسابات :

POST /loq/find_users HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: DFB2CC57-E511-4C3D-B5C3-2A324F4ABB45
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn

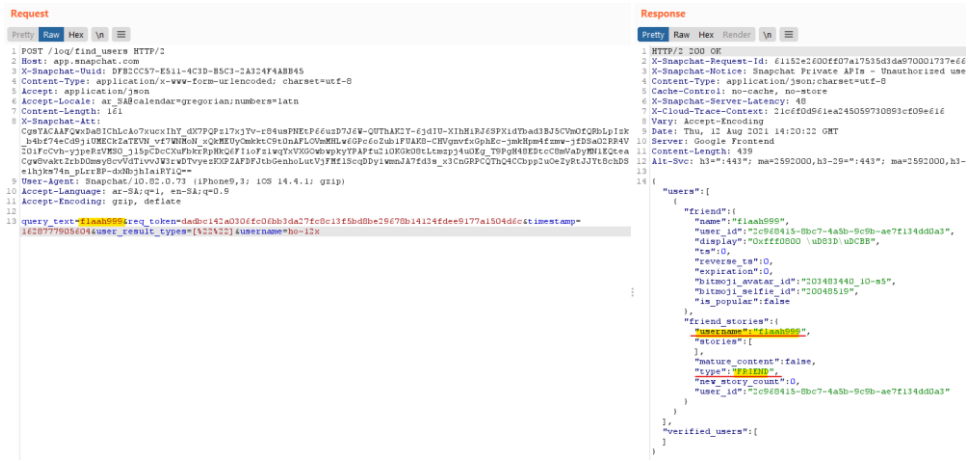
II7MAD99@GMAIL.COM 26 Oct 2021

Content-Length: 161
X-Snapchat-Att: CgsYACAAFQwxDa8IChLcAo7xucxIhY_dX7PQPzl7xjYv-r84usPNEtP66uzD7J6W-QUThAK2Y-6jdIU-XIhHiRJ6SPXidYbad3BJ5CVm0fQRbLpIzk_b4bf74eCd9jiUMECkZaTEVN_vf7WNMoN_xQkMEUyOmkktC9t0nAFLOVmMHLw6GPc6oZub1FUAK8-CHVgnvfxGphEc-jmkHpm4fzmw-jfDSa02RR4V20iFcCvh-yjpeRzVMS0_jl5pCDcCXuFbkrRpHkQ6FIioFz1wqYxVXGOwbwpkyYPAPfu2i0KGk08tLtmzpj4u0Eg_T9PgH48EDtcC8mVaDyMN1EQteaCgw8vaktZrbD0msy8cvVdTivvJW3rwDTvyezKXPZAFDFJtbGenhoLutVjFMflScqDDy1wmnJA7fd3s_x3CnGRPCQThQ4CCbpp2uOeZyRtJJYt8chDSe1hjks74n_pLrrBP-dxNbjhIaiRY1Q==
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

query_text=flaah999&req_token=dadbc142a0306fc06bb3da27fc8c13f5bd8be29678b14124fdee9177a1504d6c&timestamp=1628777905604&user_result_types=[%22%22]&username=ho-12x

تلاحظ كلمة query_text وتعني ابحث لي عن حساب flaah999 للمعلومية تقدر تبحث عن أي حساب بنفس الطلب بمجرد تغير flaah999 الي الحساب الي تبيه

نشوف رد السيرفر يوم طلبت استعلم عن الحساب:



"type":"FRIEND"اذا شفت الكلمة اعرف صاحب الحساب يتابعك وانت تتابعه

طيب لو كان ما يتابعني ولا اتابعه راح يكون الرد :

{"users":[{"friend":{"name":"foo","user_id":"fb32df3b-cc6a-4a2d-9f0b-a3bc01c29013","display":"FOO","ts":0,"reverse_ts":0,"expiration":0,"is_popular":true}}],"verified_users":[]}

ماراح تشوف كلمة friend_stories ويعني الحساب مايتابعك ولا انت تتابعه
عكس يوم يكون يتابعك راح يطلع

II7MAD99@GMAIL.COM 26 Oct 2021

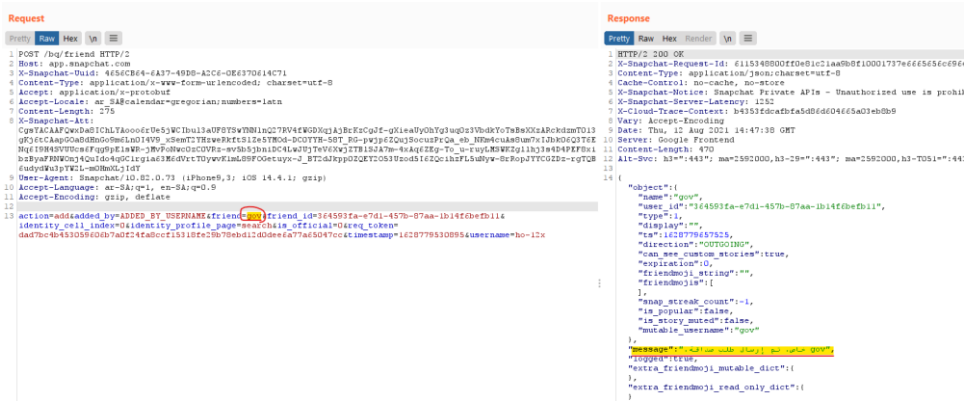
"friend_stories":{"username":"flaah999","stories":[],"mature_content":false,"type":"FRIEND"

طلب متابعه حساب :

```
POST /bq/friend HTTP/2
Host: app.snapchat.com
X-Snapchat-Uuid: 4656CB64-6A37-49D8-A2C6-0E6370614C71
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/x-protobuf
Accept-Locale: ar_SA@calendar=gregorian;numbers=latn
Content-Length: 275
X-Snapchat-Att:
CgsYACAAFQwxDa8IChLYAooo6rUe5jWCIbul3aUF8YSwYNNlnQ27RV4fWGDXqjAjBrKzCgJf-
gXieaUy0hYg3uq0z3VbdkYoTsBsXXzARckdzmT013gKj6tCAapGOa8dHnGo9m6Ln0I4V9_xSemT2YHz
weRkftSlZe5YMOd-DC0YYH-58T_RG-
pwjp6ZQujSocuzPrQa_eb_NKm4cuAs8um7xIJbk06Q3T6ENq6I9H4SVUUcs6Fqg9pElsWR-
jMvPoNwc0zC0VRz-sv5b5jbniDC4LwJUjTeV6XwjZTBlSJA7m-4xAq6ZEg-To_u-
ruyLMSWKZgllhj3s4D4PEF8xibzByaFRNWOnj4QuIdo4qGC1rgia63M6dVrtT0ywvK1mL89FOGetuyx-
J_BT2dJkpp0ZQEY2O53Uzod5I6ZQcihzFL5uNyw-8rRopJYYCGZDz-rgTQB6udydWu3pYW2L-
m0HmXLjIdY
User-Agent: Snapchat/10.82.0.73 (iPhone9,3; iOS 14.4.1; gzip)
Accept-Language: ar-SA;q=1, en-SA;q=0.9
Accept-Encoding: gzip, deflate

action=add&added_by=ADDED_BY_USERNAME&friend=gov&friend_id=364593fa-e7d1-457b-
87aa-
1b14f6befb11&identity_cell_index=0&identity_profile_page=search&is_official=0&req_token=da
d7bc4b453059606b7a0f24fa8ccf15318fe29b78ebd12d0dee6a77a65047cc&timestamp=162877953
0895&username=ho-12x
```

طلبت اتابع حساب gov نشوف رد السيرفر:

II7MAD99@GMAIL.COM 26 Oct 2021



"message":"خاص. تم إرسال طلب صداقة. gov"
"logged":true,"extra_friendmoji_mutable_dict":{},"extra_friendmoji_read_only_dict":{},"
}

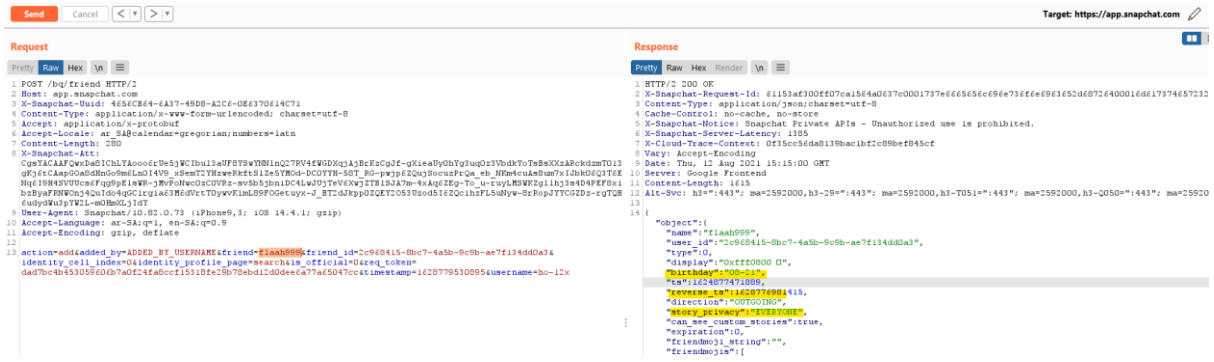
إذا كنت تريد اضافه حساب اخر من نفس الطلب عندك حاجتين لازم تغيرها من الداتا هي:

action=add&added_by=ADDED_BY_USERNAME&friend=flaah999&friend_id=2c968415-8bc7-4a5b-9c9b-ae7f134dd0a3&identity_cell_index=0&identity_profile_page=search&is_official=0&req_token=dad7bc4b453059606b7a0f24fa8ccf15318fe29b78ebd12d0dee6a77a65047cc&timestamp=1628779530895&username=ho-12x

تلاحظ عندك friend_id ويعني id الحساب لازم تبدله الي الحساب الي تبي تضيفه وطريقة استخراج id الحساب يكون من خلال البحث في خانه الإضافات في سناب شات ومثل ما شرحت في صفحة 70 من عند user_id

بخصوص friend يعني اسم المستخدم الي راح تضيفه

اذا تم قبول الإضافة راح تعرف تفاصيل اضافيه مثل تاريخ شهر الميلاد واليوم حساب عام او خاص وتاريخ اخر تسجيل الدخول



display":"0xfff0800 ","birthday":"08-"
,"21","ts":1624877471889,"reverse_ts":1628776981415,"direction":"OUTGOING","story_privacy":"EVERYONE

يعني birthday تاريخ الميلاد 08/21 بخصوص reverse_ts الوقت انسخ اول 10 مثل عندك راح يطلع 1628776981415 احذف اخر 3 ارقام راح يكون 1628776981 وطريقة الاستعلام عن الوقت من خلال موقع www.epochconverter.com

II7MAD99@GMAIL.COM 26 Oct 2021

مثل ما شرحت في صفحة 67/66 بخصوص story_privacy ويعني حالة الحساب خاص او عام إذا ما طلعت لك يعني الحساب خاص

فحص تطبيق Instagram من Mitmproxy

رجع اصدار تطبيق الإنستغرام الي 159.0

نحتاج ثبيت أداة من Cydia من السورس *https://build.frida.re*
اسم الأداة Frida إذا تم تنزيلها عندك في الجهاز تحتاج توصل جهازك الي الكمبيوتر من خلال سلك USB

ملاحظه تم تجربة Frida من خلال جهاز لينكس وماك فقط

الان تحتاج تثبت Frida عندك في الكمبيوتر من محطة الترمينال
تثبيت frida: `pip install frida-tools`
تثبيت MEDUZA : `git clone https://github.com/kov4l3nko/MEDUZA`
ملاحظة الرجاء حفظ ملف MEDUZA في سطح المكتب او نقله الي سطح المكتب بعد تنزيله
الان نحتاج تنزيل Mitmproxy عشان نستطيع فحص البرامج من خلاله بديل Burp Suite
ملاحظة تم التجربه على جهاز Windows وعلى نظام Kali Linux بنظام الوهمي بوقت واحد

رابط تنزيل Mitmproxy إذا كان جهازك Linux: `https://mitmproxy.org`
إذا كان جهازك Mac اكتب في محطة الترمينال: `brew install mitmproxy`
رابط تنزيل Mitmproxy إذا كان جهازك Windows: `https://mitmproxy.org`

تعليمات اضافيه: https://docs.mitmproxy.org/stable/overview-installation

إذا تم تنزيل Mitmproxy بنجاح تحتاج ربط جهازك الايفون في الأداة مثل Burp Suite

من خلال الاعدادات ثم wi-fi ثم علامة التعجب ثم تكوين الملقم واختيار يدويا
الخادم تكتب Ip الكمبيوتر المثبت عليه أداة Mitmproxy و البورت 8080

استخراج Ip الكمبيوتر من خلال محطة الترمينال mac,linux : `ifconfig | grep "inet"`
استخراج Ip الكمبيوتر من خلال محطة الترمينال Windows : `ipconfig`

II7MAD99@GMAIL.COM 26 Oct 2021

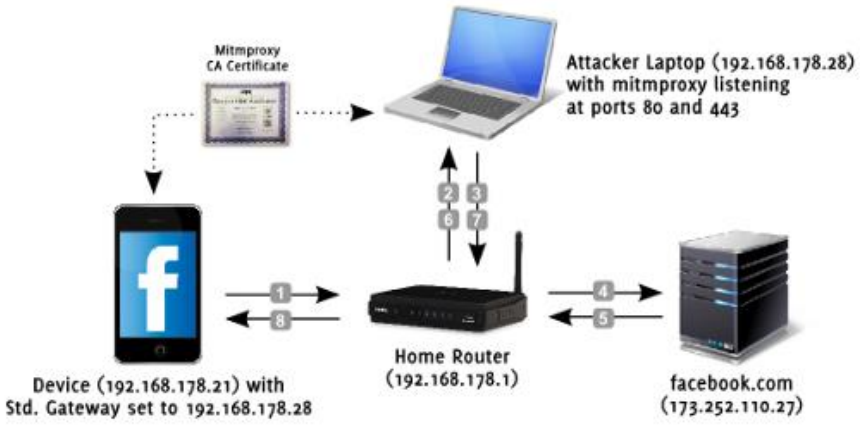

```
falah — -zsh — 101×24
falah@MacBook-Pro-alkhas-b-FaLaH ~ % ifconfig | grep "inet"
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet6 fe80::e0:ce63:d388:2c42%en1 prefixlen 64 secured scopeid 0x7
        inet 192.168.100.16 netmask 0xffffff00 broadcast 192.168.100.255
        inet6 fe80::69fe:753c:24de:6f42%utun0 prefixlen 64 scopeid 0xb
        inet6 fe80::54de:4cf7:86e7:3b53%utun1 prefixlen 64 scopeid 0xc
        inet6 fe80::1032:171f:bc2e:5d1a%en4 prefixlen 64 secured scopeid 0xe
        inet 169.254.88.60 netmask 0xffff0000 broadcast 169.254.255.255
falah@MacBook-Pro-alkhas-b-FaLaH ~ %
```

بعد ربط الايبي و البورت في جهازك الايفون اكتب في محطة الترمينال الكمبيوتر : Mitmproxy
تلاحظ تم تشغيل الأداة

```
falah — Mitmproxy — 101×24
Flows
>>03:44:50 HTTPS GET  …unes.apple.com /itunes-assets/Purple125/v4… 206 …n/octet-stream 3.56m 1.34s
  03:44:50 HTTPS GET  …unes.apple.com /itunes-assets/Purple125/v4… 206 …ntent missing]
  03:44:50 HTTPS GET  …unes.apple.com /itunes-assets/Purple125/v4… 206 …ntent missing]

[1/3]                                                                  [*:8080]
```

الان نحتاج ربط الشهادة الخاصه في Mitmproxy في الجهاز الايفون الذي تم ربطه سابقا

II7MAD99@GMAIL.COM 26 Oct 2021



نكتب في المتصفح: mitm.it

ثم تنزيل ملف التعريف ثم نذهب الاعدادات ونوثقه مثل الخطوات السابقه في ربط شهادة Burp Suite
الان تستطيع فحص تطبيق الانستغرام من خلال Mitmproxy

الان افتح بمحطة جديدة الترمينال واكتب :

١. cd Desktop
٢. cd MEDUZA
٣. cd scripts
٤. python3 meduza.py -s com.burbn.instagram ./unpinUber.js

II7MAD99@GMAIL.COM 26 Oct 2021


```
Parrot Terminal
File Edit View Search Terminal Help
┌─[falah@parrot]─[~/Desktop/MEDUZA-master/scripts]
└──╼ $python3 meduza.py -s com.burbn.instagram ./unpinUber.js
MEDUZA iOS SSL unpinning tool
by Dima Kovalenko (@kov4l3nko)
==========================================================

[*] Waiting for an iOS device connected to USB...
[*] Spawning com.burbn.instagram...
[*] Attaching to com.burbn.instagram...
[*] Reading JS payload meduza.js...
[*] Injecting JS payload to the process...
[*] SecCertificateCreateWithBytes(...) hooked!
[*] Resuming the application...
[*] Press ENTER to complete (you can do it anytime)...
[*] Got another certificate, its raw SHA256 hash: 17148253ca119b78759b4e11321d69
0a061668ce39a23ce14085f40609d7fc7f
        *.facebook.com
        *.xy.fbcdn.net
        *.fbcdn.net
        facebook.com
        *.messenger.com
        messenger.com
        *.facebook.net
        graph.facebook.com
        *.m.facebook.com
        *.fbsbx.com
        *.xz.fbcdn.net
        *.xx.fbcdn.net
[*] Got another certificate, its raw SHA256 hash: d56d69fc8241c00dd448ac6e08416e
fc8e909eec2d6f70764e9350bee6b57b01
```

تلاحظ كاتب لك `s- com.burbn.instagram`
ويعني فك لي التشفير التطبيق الانستغرام من خلال الدايلب

طيب كيف اجيب دايلب تطبيق ثاني ؟

كتابة في الترمينال : `python3 meduza.py -l`

او من خلال Frida: `frida-ps -Uai`

للتوضيح شاهد الصورة التالية

II7MAD99@GMAIL.COM 26 Oct 2021


```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
┌─[falah@parrot]─[~]
└──╼ $frida-ps -Uai
PID  Name            Identifier
----  ---------------  ------------------------------------
1993  Snapchat         com.toyopagroup.picaboo
   -  Al Rajhi Mobile  sa.alrajhibank.retailapp
   -  App Store        com.apple.AppStore
   -  Apps Manager     com.tigisoftware.ADManager
   -  BIGO LIVE        sg.bigo.live
   -  Between          kr.co.vcnc.couple
   -  Brain Test 2     com.unicostudio.braintest2
   -  Chrome           com.google.chrome.ios
   -  Cydia            com.saurik.Cydia
   -  Duo Mobile       com.duosecurity.DuoMobile
   -  ESign            rl.esign.YYYSign.co
   -  FaceTime         com.apple.facetime
   -  Filza            com.tigisoftware.Filza
   -  Gmail            com.google.Gmail
   -  Google Maps      com.google.Maps
   -  HotspotShield    com.anchorfree.hss
   -  HungerStation    com.hungerstation.ios.hungerstationapp
   -  ImageSearch      com.ipopapp.imagesearchfree
   -  Instagram        com.burbn.instagram
   -  Jahez            com.alamat.jahez
   -  Layout           com.burbn.layouts
   -  LibTerm          ch.marcela.ada.LibTerm
   -  MEGA             mega.ios
```

تبدل الدايلب `com.burbn.instagram` الي الدايلب التطبيق الاخر
مثال دايلب تطبيق **Mega** هو: mega.ios

يكون الامر: `python3 meduza.py -s mega.ios ./unpinUber.js`

طريقة MEDUZA المذكورة تفتح لك تشفير بعض التطبيقات من خلال الدايلب

إذا لم يفتح تشفير الإنستغرام تحتاج خطوة ثانيه مضمونه وهي unpin-ssl-instagram-ios-159.0.js

من خلال أداة Frida تابع الخطوات التالية:

١. تحتاج تنزيل ملف unpin-ssl-instagram-ios-159.0.js من https://github.com/kov4l3nko/InstagramSSLPinningBypass-iOS/tree/master/script

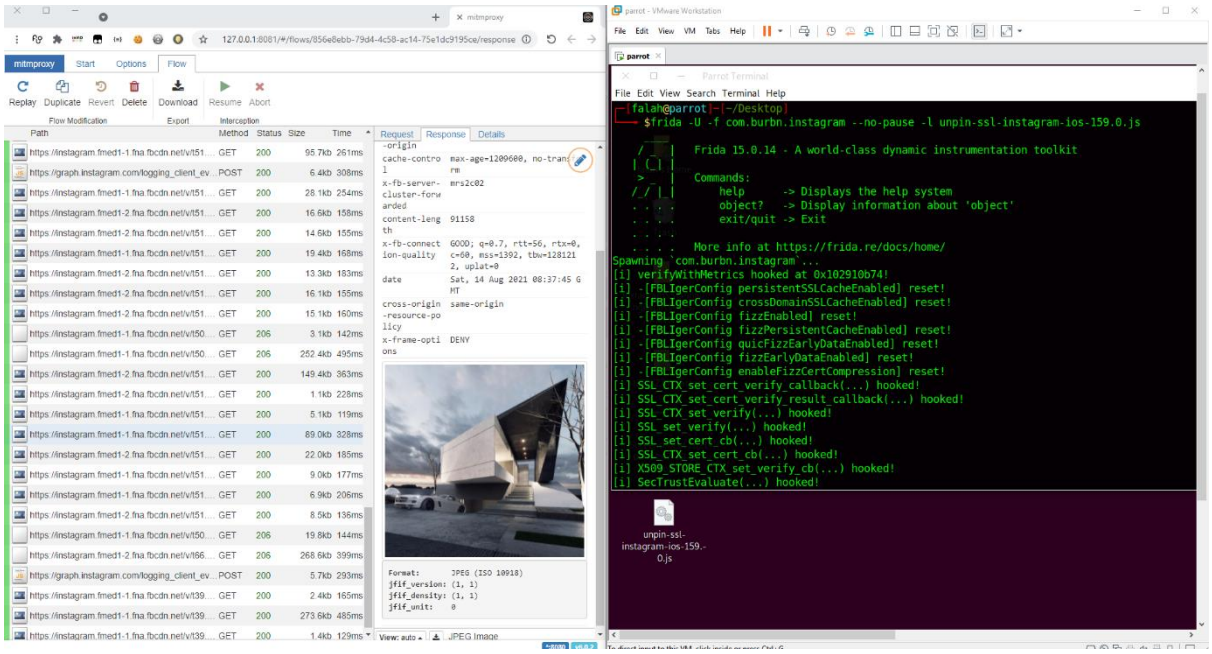
٢. عند الدخول على الرابط سوف تشاهد ملف ينتهي 159.0.js و 157.0.js ويعني الإصدار تطبيق الانستغرام انا حملت 159.0.js لأني رجعت الإصدار التطبيق الي 159.0

٣. بعد تحميله وضعته على سطح المكتب وكتبت الامر التالي

frida -U -f com.burbn.instagram --no-pause -l unpin-ssl-instagram-ios-159.0.js

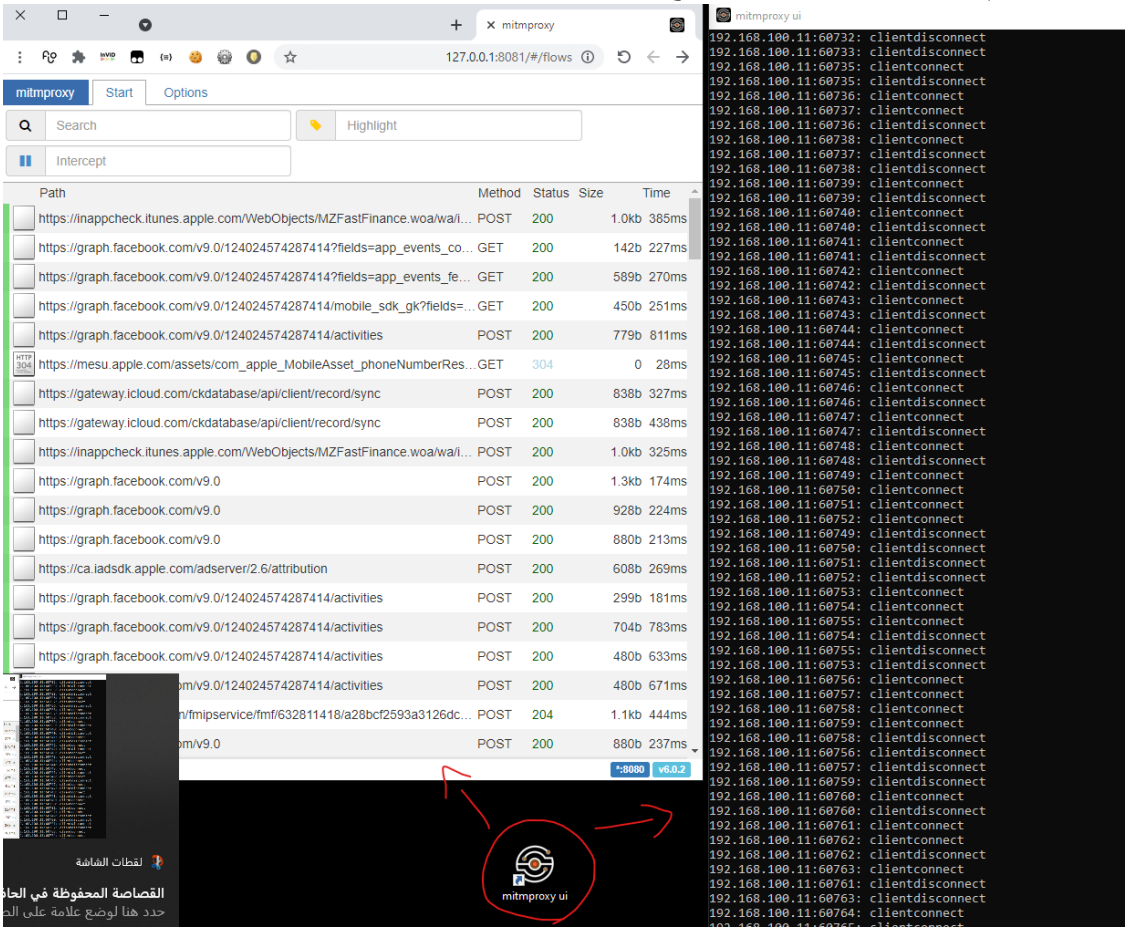
II7MAD99@GMAIL.COM 26 Oct 2021

النتيجة:



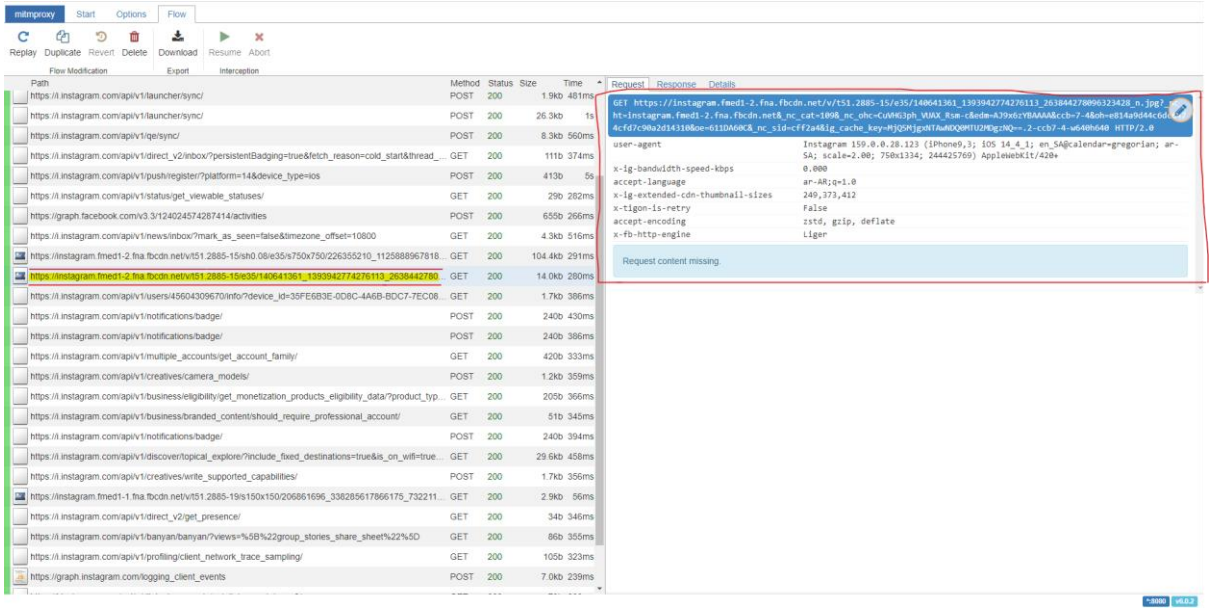
تم فك تشفير instagram من خلال أداة Frida

برنامج Mitmproxy على الويندوز مختلف تماما عن اللينكس والماك
الفرق بينهم انه على الويندوز كبرنامج وليس أداة



II7MAD99@GMAIL.COM 26 Oct 2021

تلاحظ عند الضغط على البرنامج Mitmproxy ui سوف تشاهد فتح صفحة على الويب والترمينال على الويب تشاهد عرض الطلبات عند الضغط على الرابط او على الطلب تشاهد انقسام الشاشة الي جزئين جزء فيه الطلبات بنفس الصفحة وجزء فيه بيانات الطلب مثل:



على اليمين فيها بيانات الطلب وتلاحظ في الشريط ثلاث خيارات

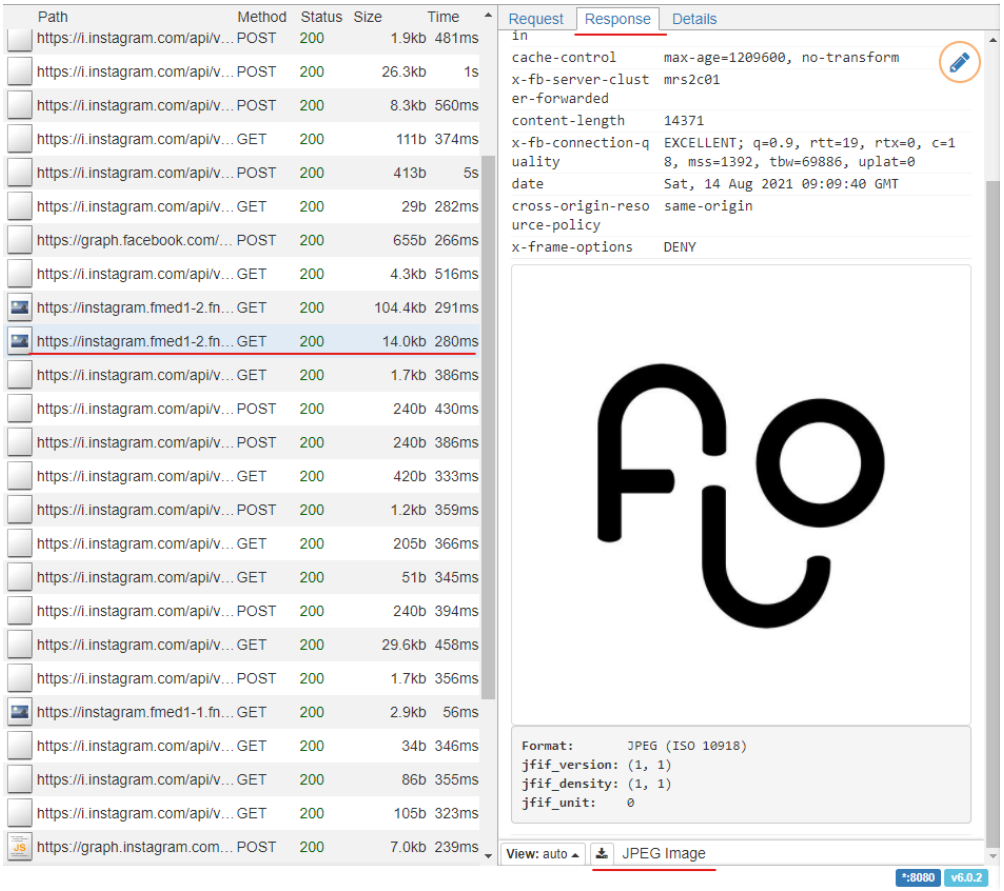
- **Request - Response - Details**

١. Request فيها بيانات الطلب مثل نوع الجهاز والاصدار و الرابط الطلب و الداتا
٢. Response فيها رد السيرفر للملاحظة ما نقدر نعدل البيانات في البرنامج mitmproxy
٣. Details فيها الوقت الطلب مع الرد السيرفر وغيرها

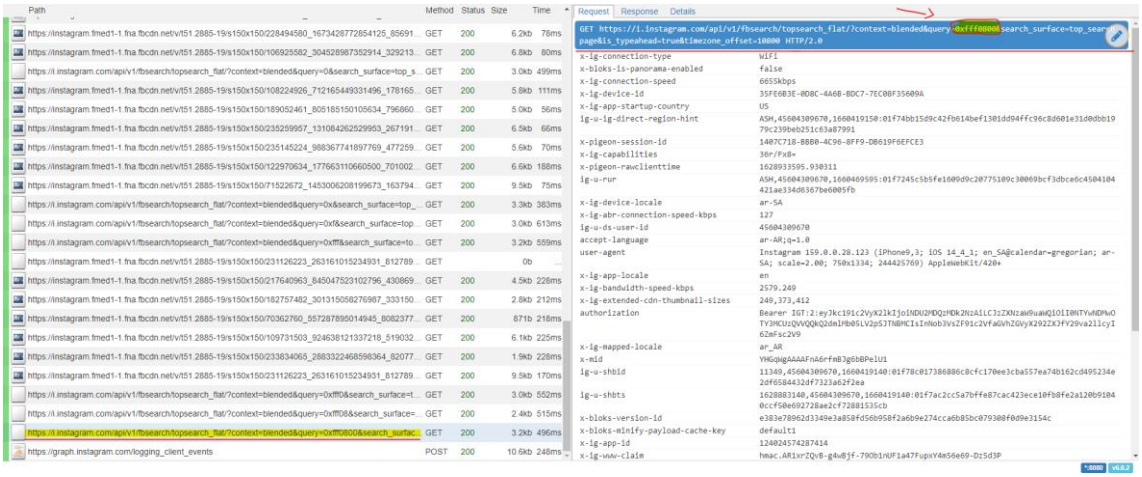
نفس خيارات الماك ولينكس

II7MAD99@GMAIL.COM 26 Oct 2021

مثال إذا ضغطنا على Response نشاهد الصورة ونستطيع حفظها:



مثال ثاني دخلت تطبيق الانستغرام وسويت بحث عن 0xfff0800 وكانت النتيجة:



II7MAD99@GMAIL.COM 26 Oct 2021

عند ما ضغطت Response عشان اشوف رد السيرفر:

Request | Response | Details


```
{
    "clear_client_cache": null,
    "has_more": true,
    "list": [
        {
            "position": 0,
            "user": {
                "account_badges": [],
                "follow_friction_type": 0,
                "friendship_status": {
                    "following": false,
                    "incoming_request": false,
                    "is_bestie": false,
                    "is_private": false,
                    "is_restricted": false,
                    "outgoing_request": false
                },
                "full_name": "فلاح العنزي",
                "has_anonymous_profile_picture": false,
                "is_private": false,
                "is_verified": false,
                "latest_reel_media": 0,
                "live_broadcast_id": null,
                "pk": 1028900743,
                "profile_pic_id": "2396580633913712657_1028900743",
                "profile_pic_url": "https://instagram.fmed1-1.fna.fbcdn.net/v/t51.2885-19/s150x150/119462120_625949664960229_52
                "search_social_context": "Followed by o_o12393",
                "social_context": "Followed by o_o12393",
                "username": "0xfff0800"
            }
```



```
"full_name": "فلاح العنزي",
"has_anonymous_profile_picture": false,
"is_private": false,
"is_verified": false,
"latest_reel_media": 0,
"live_broadcast_id": null,
"pk": 1028900743,
"profile_pic_id": "2396580633913712657_1028900743",
"profile_pic_url": "https://instagram.fmed1-1.fna.fbcdn.net/v/t51.2885-19/s150x150/119462120_625949664960229_5297275746054404499_n.jpg?_nc_ht=instagram.fmed1-1.fna.fbcdn.net&_nc_ohc=tjySKZhl4U8AX-KL88C&edm=AP9-OL4BAAAA&ccb=7-4&oh=4d862c7f11cb3786e7cbb4699b8cc7e0&oe=611E8C76&_nc_sid=737f18",
"search_social_context": "Followed by o_o12393",
"social_context": "Followed by o_o12393",
"username": "0xfff0800"
```


طلب تسجيل دخول: POST https://i.instagram.com/api/v1/accounts/login/

II7MAD99@GMAIL.COM 26 Oct 2021

Request Response Details

POST https://i.instagram.com/api/v1/accounts/login/ HTTP/2.0

x-ig-connection-speed	2035kbps
content-length	758
x-ig-device-id	35FE6B3E-0D8C-4A6B-BDC7-7EC08F35609A
x-ig-app-startup-country	US
x-ig-capabilities	36r/Fx8=
x-ig-device-locale	ar-SA
x-ig-abr-connection-speed-kbps	112
accept-language	ar-AR;q=1.0
user-agent	Instagram 159.0.0.28.123 (iPhone9,3; iOS 14_4_1; en_SA@calendar=gregorian; ar-SA; scale=2.00; 750x1334; 244425769) AppleWebKit/420+
content-type	application/x-www-form-urlencoded; charset=UTF-8
x-ig-app-locale	en
x-ig-extended-cdn-thumbnail-sizes	249,373,412
x-ig-bandwidth-speed-kbps	96.879
x-ig-mapped-locale	ar_AR
x-mid	YHGqWgAAAAFnA6rfmBJg6bBPelU1
x-bloks-is-panorama-enabled	false
x-bloks-version-id	e383e78962d3349e3a858fd56b958f2a6b9e274cca6b85bc079308f0d9e3154c
x-bloks-minify-payload-cache-key	default1
x-ig-app-id	124024574287414
x-ig-connection-type	WiFi
x-tigon-is-retry	False
accept-encoding	zstd, gzip, deflate
x-fb-http-engine	Liger

signed_body: SIGNATURE.{"username":"test99912","reg_login":"0","enc_password":"#PWD_INSTAGRAM:4:1628934436:AYlOxvgVeHXISnmFO5IA

View: auto URLEncoded form

الداتا :


```
SIGNATURE.{"username":"test99912","reg_login":"0","enc_password":"#PWD_INST
AGRAM:4:1628934436:AYlOxvgVeHXISnmFO5IAAUEokKu2v6u0wN19PM+7mPH5ZNmrOUTOADmp
ytPNtO\/6GeVcm+TAXbs6pFIPYiKmQ28th+Vtqz6rkrX9zFzbguvghLFkJeQ99VyaTZIavr9bdC
VE4+FD\/H056fisHS2ILF1uml\/0yqrxWIynVSDlj49bEWX5P69UuPZgIZqa5igHWspiM5QHxaD
LnzGLSHkgZa69N9RHr2vKgA+My0qye7ZzvBubZZLfQ+hCT4PDdsfKsHjDboH6AYQdPl3gB+ebrz
Pm0gq+a9\/jho7I2WF4GeBJ2u4AZNGKk05ricLwwhFqRuxTC5nyVSglQkSjqMZ4olyXT\/HDyy3
1+A2zlOcrGETxbqNjSy9oHdyC1yFT5aOhLaZ0tvCrZdc=","device_id":"35FE6B3E-0D8C-
4A6B-BDC7-7EC08F35609A","login_attempt_count":"0","phone_id":"35FE6B3E-
0D8C-4A6B-BDC7-7EC08F35609A"}
```


تلاحظ password مشفر بتشفيره evp_aes_256_gcm في الإنستغرام

راجع مصدر:

https://stackoverflow.com/questions/62436766/cant-login-to-instagram-using-requests

II7MAD99@GMAIL.COM 26 Oct 2021

رد السيرفر:

```
{
    "buttons": [
        {
            "action": "dismiss",
            "title": "Try Again"
        }
    ],
    "error_title": "Incorrect password for test99912",
    "error_type": "bad_password",
    "invalid_credentials": true,
    "message": "The password you entered is incorrect. Please try again.",
    "status": "fail"
}
```

تسجيل الدخول فشل لأنني لم اضع كلمة مرور الصحيحه التابعة للحساب

استخراج الاميل والرقم مشفر من خلال نسيان كلمة المرور من داخل التطبيق:

```
https://i.instagram.com/api/v1/users/lookup/
```

الداتا

```
signed_body: SIGNATURE.{"phone_id":"35FE6B3E-0D8C-4A6B-BDC7-
7EC08F35609A","device_id":"35FE6B3E-0D8C-4A6B-BDC7-
7EC08F35609A","q":"test99912","country_codes":"[{\"country_code\":\"966\",\
"source\":[\"default\"]}]","waterfall_id":"a0cb56df45f84eef9cb2dbe6a908d581
"}
```

الحساب الي سويت له نسيان كلمة مرور: test99912

II7MAD99@GMAIL.COM 26 Oct 2021

رد السيرفر:


```
{
    "can_email_reset": true,
    "can_sms_reset": true,
    "can_wa_reset": false,
    "corrected_input": "test99912",
    "email": "test99912",
    "email_sent": false,
    "fb_login_option": false,
    "has_valid_phone": true,
    "lookup_source": "username",
    "multiple_users_found": false,
    "obfuscated_email": "f*******1@gmail.com",
    "obfuscated_phone": "+966 ** *** **36",
    "phone_number": "test99912",
    "sms_sent": false,
    "status": "ok",
    "user": {
        "account_badges": [],
        "follow_friction_type": -1,
        "full_name": "",
        "has_anonymous_profile_picture": true,
        "is_private": false,
        "is_verified": false,
        "pk": 45604309670,
        "profile_pic_url": "https://scontent-frx5-1.cdninstagram.com/v/t51.2885-19/44884218
_345707102882519_2446069589734326272_n.jpg?_nc_ht=scontent-frx5-1.cdninstagram.com&_nc_ohc=
ZLFK6RFNcgAAX9aH5K6&edm=AD35FJ8BAAAA&ccb=7-4&oh=4c47781a00311b7ee2a2a8dc04794c6b&oe=611DBE8
F&_nc_sid=74408c&ig_cache_key=YW5vbnltb3VzX3Byb2ZpbGVfcGlj.2-ccb7-4",
        "username": "test99912"
    },
    "user_id": 45604309670
}
```

II7MAD99@GMAIL.COM 26 Oct 2021

تفكيك التطبيقات واستخراج ملفاتها

١. تحتاج تثبيت Frida على الكمبيوتر والايفون
٢. تنزيل أداة: https://github.com/AloneMonkey/frida-ios-dump
الرجاء حفظ الملف على سطح المكتب
٣. تحميل أداة openssh من Cydia في جهازك الايفون

من أسهل الطرق لا تفكيك التطبيق وقراءة ملفاته من خلال اسم التطبيق والدايلب فقط

(الهندسة العكسية للتطبيقات -Reverse Engineering)

على الرغم من وجود العديد من منشورات المدونات والبرامج التعليمية وحتى مقاطع فيديو YouTube حول "تطبيقات الهندسة العكسية لنظام iOS" ، في كل مرة تصدر Apple إصدارًا جديدًا من نظام التشغيل iOS ، وتتغير "اللعبة" ؛ يتعين على الباحثين إيجاد طريقة جديدة لكسر حماية الإصدار الجديد من نظام التشغيل iOS وعلينا تحديث أدواتنا للعمل مع بيئة الجيلبريك الجديدة .هذا ينطبق بشكل خاص على أحدث جيلبريك iOS 15 ، كل من LiberiOS و jailbreaks Electra، والتي تستند إلى استغلال async wake Ian Beer ، لها تقنيات مختلفة تمامًا عن عمليات كسر الحماية السابقة ومعظم (كل؟) الأدوات الحالية مكسورة على هذه الجلبريك

لذلك قررت اشرح أسهل الطرق التي تعمل على جميع أنواع الجلبريك

II7MAD99@GMAIL.COM 26 Oct 2021

تشغيل أداة frida-ios-dump

نحتاج نوصل الهاتف في الكمبيوتر من خلال سلك usb
بعد تحميلها افتح محطة الترمينال ثم اكتب التالي :

1. cd DeskTop
2. cd frida-ios-dump-master
3. sudo pip install -r requirements.txt --upgrade
4. /.dump.py الدايلب -H ip -p 22

لمعرفة الدايلب للتطبيقات اكتب frida-ps -Uai :

```
┌─[falah@parrot]─[~]
└──╼ $frida-ps -Uai
 PID  Name            Identifier
----  ----------------  ----------------------------------------
1993  Snapchat         com.toyopagroup.picaboo
   -  Al Rajhi Mobile  sa.alrajhibank.retailapp
   -  App Store        com.apple.AppStore
   -  Apps Manager     com.tigisoftware.ADManager
   -  BIGO LIVE        sg.bigo.live
   -  Between          kr.co.vcnc.couple
   -  Brain Test 2     com.unicostudio.braintest2
   -  Chrome           com.google.chrome.ios
   -  Cydia            com.saurik.Cydia
   -  Duo Mobile       com.duosecurity.DuoMobile
   -  ESign            rl.esign.YYYSign.co
   -  FaceTime         com.apple.facetime
   -  Filza            com.tigisoftware.Filza
   -  Gmail            com.google.Gmail
   -  Google Maps      com.google.Maps
   -  HotspotShield    com.anchorfree.hss
   -  HungerStation    com.hungerstation.ios.hungerstationapp
   -  ImageSearch      com.ipopapp.imagesearchfree
   -  Instagram        com.burbn.instagram
   -  Jahez            com.alamat.jahez
   -  Layout           com.burbn.layouts
   -  LibTerm          ch.marcela.ada.LibTerm
   -  MEGA             mega.ios
   -  Netflix          com.netflix.Netflix
   -  NewTerm          ws.hbang.Terminal
   -  Outlook          com.microsoft.Office.Outlook
   -  PayPal           com.yourcompany.PPClient
   -  Picsart          com.picsart.studio
```

الان نحتاج معرفة ip الايفون الي تم توصيله في الكمبيوتر من الاعدادات الايفون

II7MAD99@GMAIL.COM 26 Oct 2021

```
/.dump.py com.tmmmt.tmmmt -H 192.168.100.6 -p 22
```

انا اخترت تطبيق tmmt وكتبت الدايلب الخاص به وضعت الايبي جهازي ثم وصلت جهازي في الحاسوب

اذا فشل فك تشفير التطبيق حاول فتح التطبيق من الايفون واغلاقه من الخلفيه ثم محاولة تكرار العمليه في الحاسوب

يتم التاخير في محاوله فك تشفير التطبيق على حسب حجمه

II7MAD99@GMAIL.COM 26 Oct 2021

جاري فك التشفير

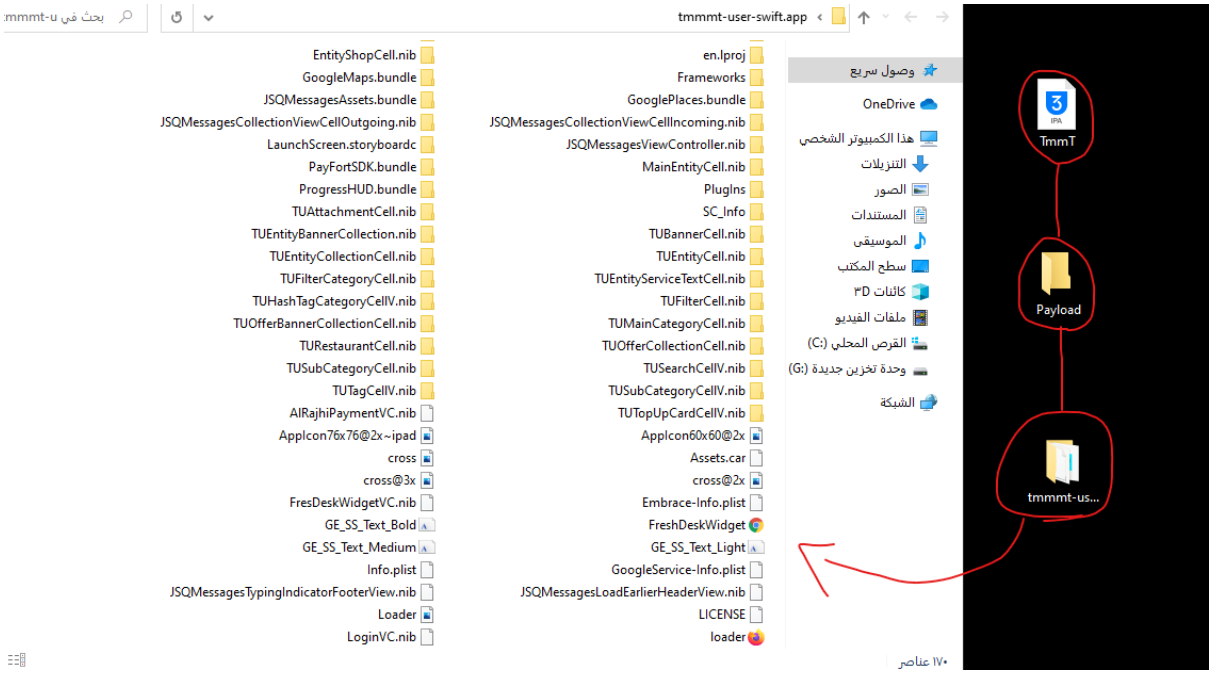
```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
┌─[falah@parrot]─[~/Desktop/frida-ios-dump-master]
└──╼ $./dump.py com.tmmmt.tmmmt -o TmmT -H 192.168.100.6 -p 22
Start the target app com.tmmmt.tmmmt
Dumping TmmT to /tmp
[frida-ios-dump]: Load OCGoogleDirectionsAPI.framework success.
[frida-ios-dump]: Load Canvas.framework success.
[frida-ios-dump]: Load FirebaseCore.framework success.
[frida-ios-dump]: Load SocketIO.framework success.
[frida-ios-dump]: Load MarqueeLabel.framework success.
[frida-ios-dump]: Load Floaty.framework success.
[frida-ios-dump]: Load GoogleToolboxForMac.framework success.
[frida-ios-dump]: Load JSONModel.framework success.
[frida-ios-dump]: Load FBLPromises.framework success.
[frida-ios-dump]: Load AWSCore.framework success.
[frida-ios-dump]: Load FirebaseInstallations.framework success.
[frida-ios-dump]: Load AFNetworking.framework success.
[frida-ios-dump]: Load FirebaseCoreDiagnostics.framework success.
[frida-ios-dump]: Load IQKeyboardManager.framework success.
[frida-ios-dump]: Load UIAlertController_Blocks.framework success.
[frida-ios-dump]: Load MBCircularProgressBar.framework success.
[frida-ios-dump]: Load QRCodeReaderViewController.framework success.
[frida-ios-dump]: Load Alamofire.framework success.
[frida-ios-dump]: Load DateTools.framework success.
[frida-ios-dump]: Load SACodedTextField.framework success.
[frida-ios-dump]: Load GoogleUtilities.framework success.
[frida-ios-dump]: Load Embrace.framework success.
[frida-ios-dump]: Load Colours.framework success.
[frida-ios-dump]: Load PINCache.framework success.
[frida-ios-dump]: Load nanopb.framework success.
[frida-ios-dump]: Load FirebaseABTesting.framework success.
[frida-ios-dump]: Load M13BadgeView.framework success.
[frida-ios-dump]: Load AWSEC2.framework success.
[frida-ios-dump]: Load FSPagerView.framework success.
[frida-ios-dump]: Load GoogleDataTransport.framework success.
[frida-ios-dump]: Load SDWebImage.framework success.
[frida-ios-dump]: Load Realm.framework success.
[frida-ios-dump]: Load GTMSessionFetcher.framework success.
[frida-ios-dump]: Load AWSSNS.framework success.
[frida-ios-dump]: Load Lottie.framework success.
[frida-ios-dump]: Load DateToolsSwift.framework success.
[frida-ios-dump]: Load FirebaseDynamicLinks.framework success.
[frida-ios-dump]: Load Protobuf.framework success.
[frida-ios-dump]: Load SkeletonView.framework success.
[frida-ios-dump]: Load MBProgressHUD.framework success.
Menu [GitHub - AloneMonkey... Parrot Terminal
```

تم فك تشفير التطبيق وحفظه بصيغة ipa في نفس مجلد الأداة

```
frida-ios-dump-master
Bookmarks Help
falah Desktop frida-ios-dump-master
dump.js   dump.py   LICENSE   process.sh   README.md   requirements.txt   TmmT.ipa
7 items, Free space: 75.1 GB

Starscream.fid: 100%|...| 502k/502k [00:00<00:00, 812kB/s]
start dump /private/var/containers/Bundle/Application/A8054E9A-5208-4D43-9DBB-E4
BFD5123B31/tmmmt-user-swift.app/Frameworks/UIAlertController_Blocks.framework/UI
AlertController_Blocks
UIAlertController_Blocks.fid: 100%|...| 91.9k/91.9k [00:00<00:00, 372kB/s]
start dump /private/var/containers/Bundle/Application/A8054E9A-5208-4D43-9DBB-E4
BFD5123B31/tmmmt-user-swift.app/Frameworks/nanopb.framework/nanopb
nanopb.fid: 100%|...| 80.1k/80.1k [00:00<00:00, 359kB/s]
objects-12.3+.nib: 76.7MB [01:36, 835kB/s]
0.00B [00:00, 7B/s]Generating "TmmT.ipa"

┌─[falah@parrot]─[~/Desktop/frida-ios-dump-master]
└──╼ $
```

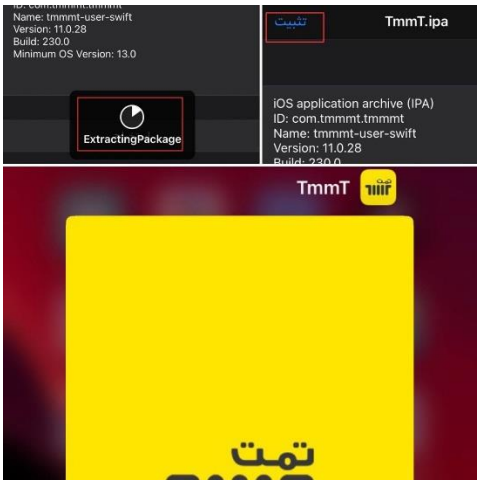
II7MAD99@GMAIL.COM 26 Oct 2021

عند فك الضغط عن ملف التطبيق سوف تشاهد مجلد باسم Payload داخل المجلد مجلد ثاني باسم البرنامج مثال tmmmt-user-swift.app داخله الملفات التطبيق بدون تشفير



إذا كنت تريد مشاركة التطبيق وتثبيته في جهاز اخر تستطيع بدون مشاكل

لتوضيح بدون فك الضغط أي مشاركة التطبيق وتثبيته من خلال Fillza بصيغة ipa بعد سحبه من أداة frida-ios-dump



II7MAD99@GMAIL.COM 26 Oct 2021

فحص Netflix من Charles

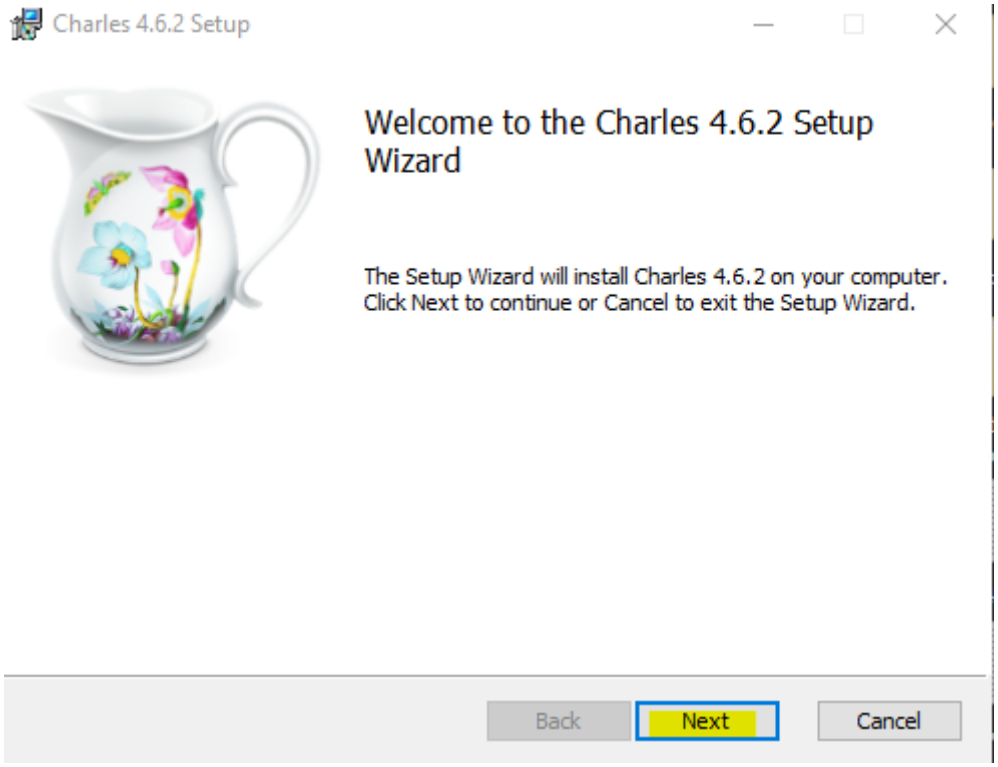
تنزيل Charles من الموقع الرسمي :

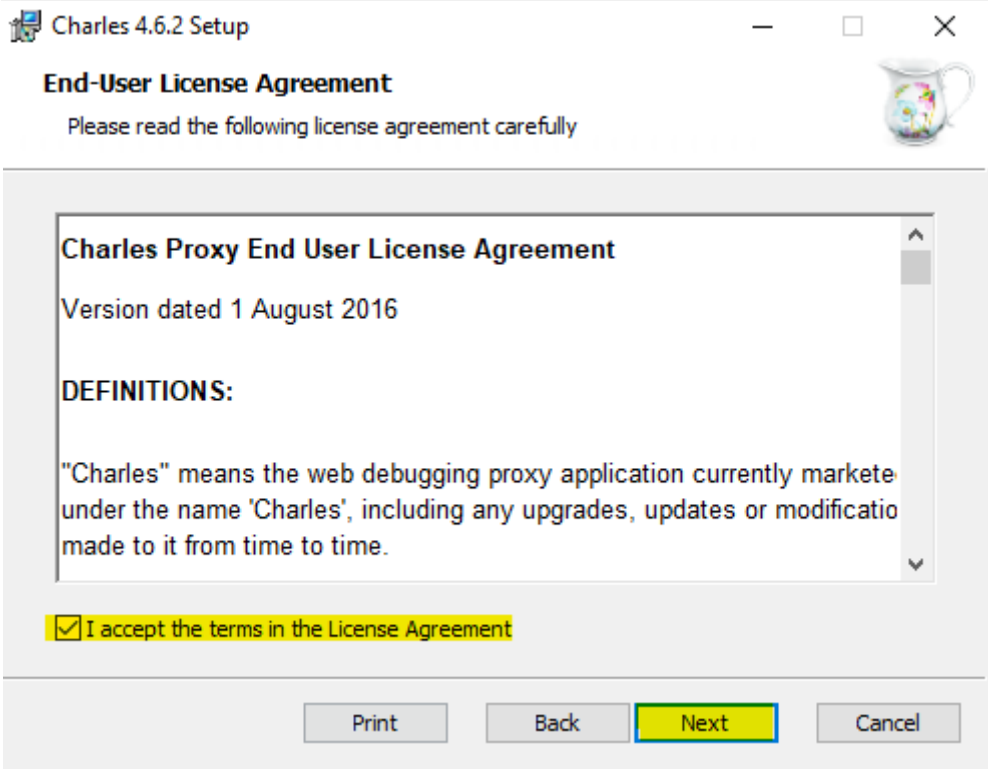
https://www.charlesproxy.com/download

متوفر على جميع أنظمة التشغيل

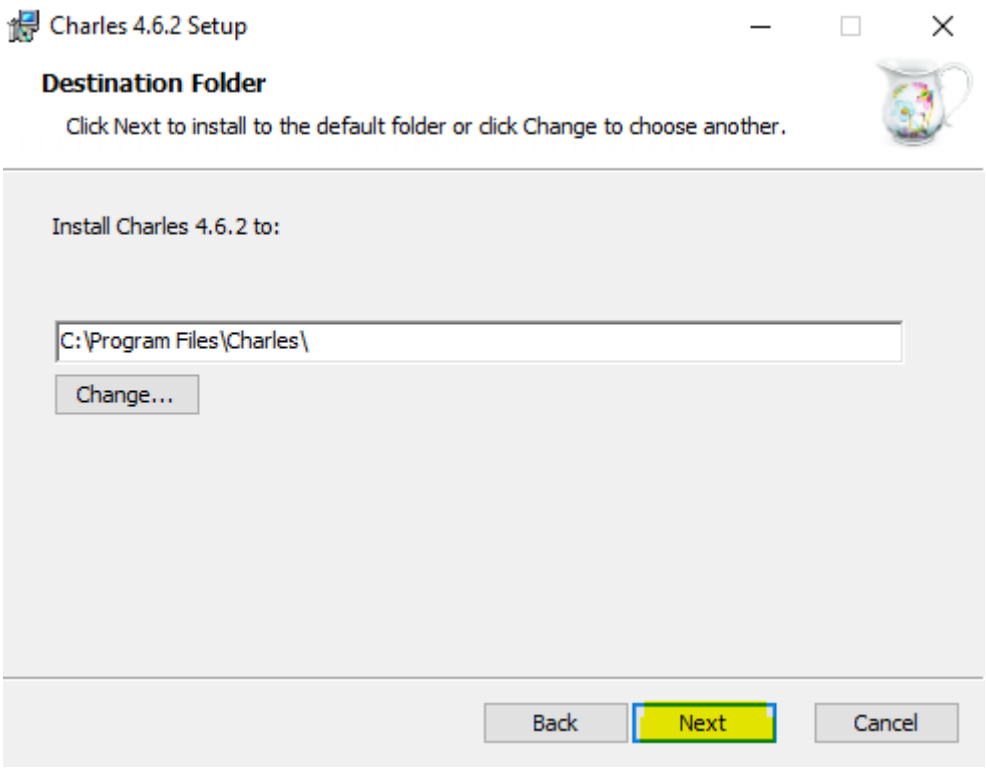
تنصيب البرنامج تابع الخطوات

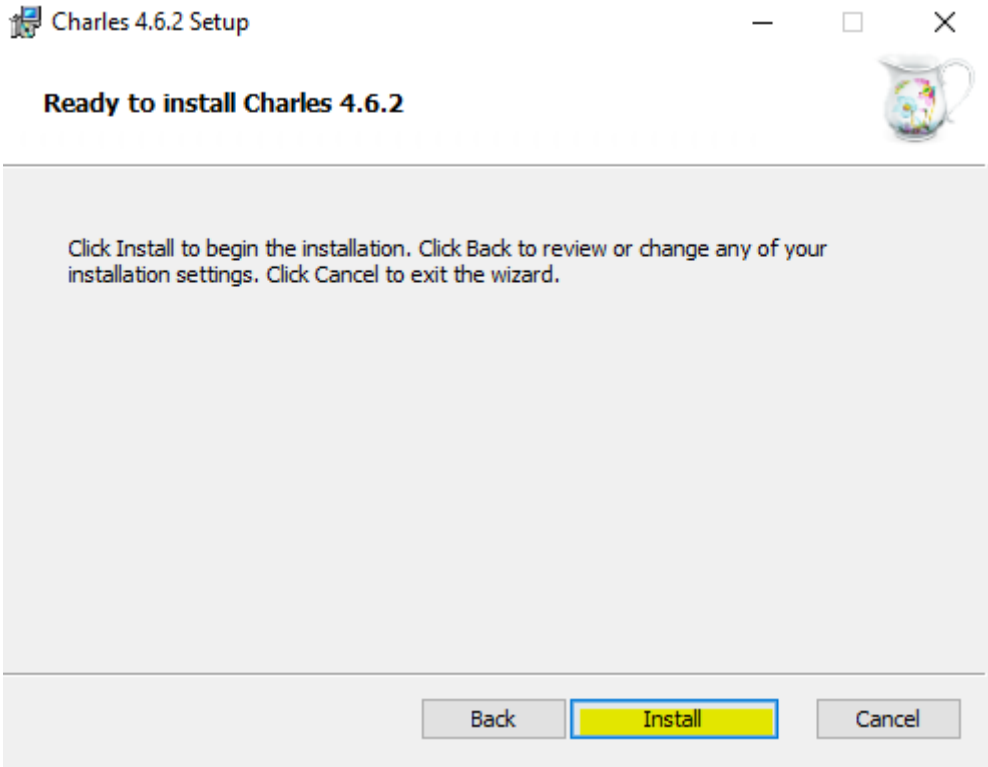
II7MAD99@GMAIL.COM 26 Oct 2021



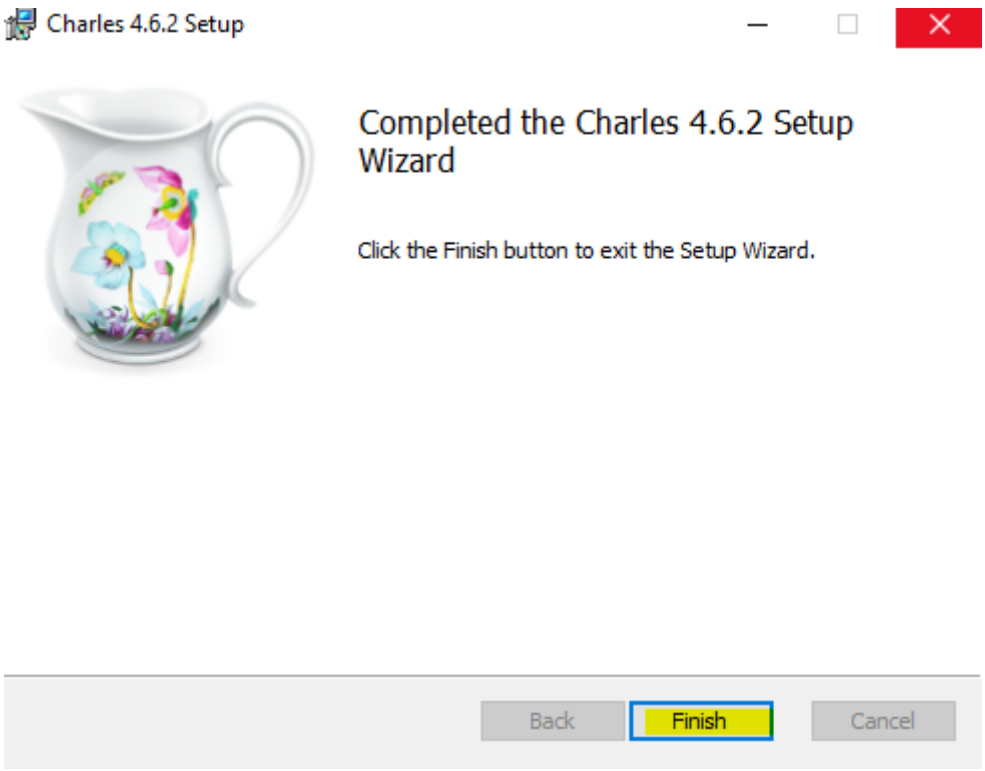


II7MAD99@GMAIL.COM 26 Oct 2021

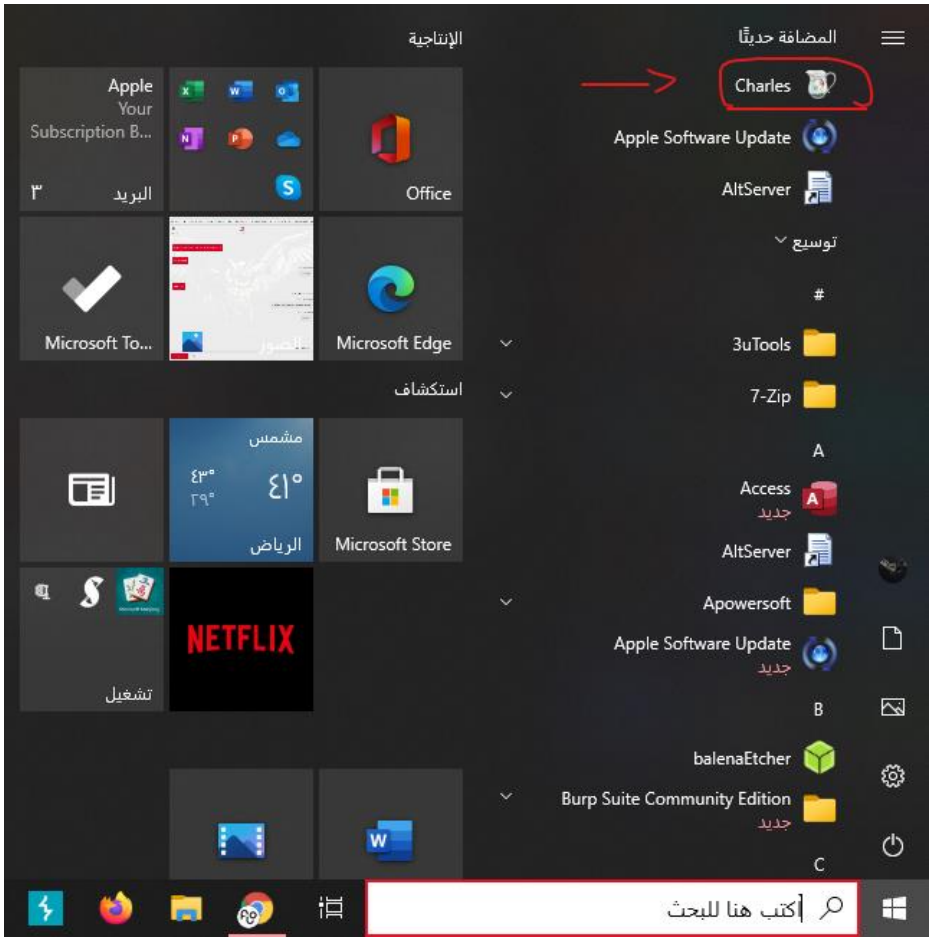




II7MAD99@GMAIL.COM 26 Oct 2021



تم تنزيل البرنامج

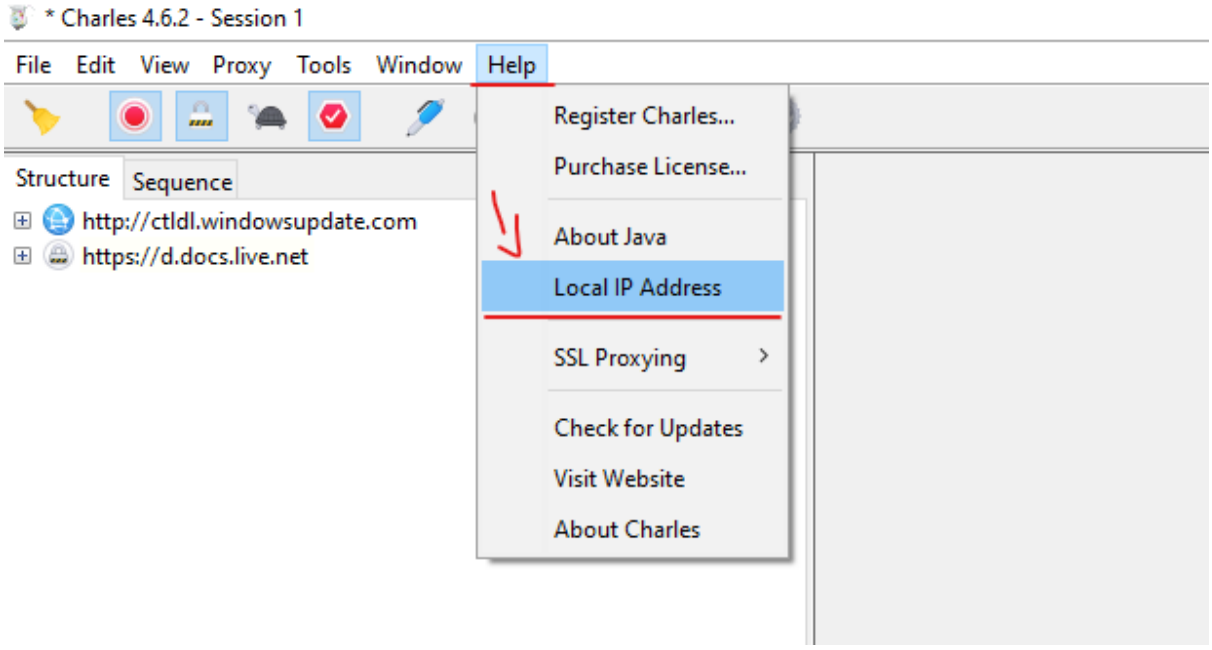


II7MAD99@GMAIL.COM 26 Oct 2021

الان تم تشغيله على الحاسوب الخاص بنا

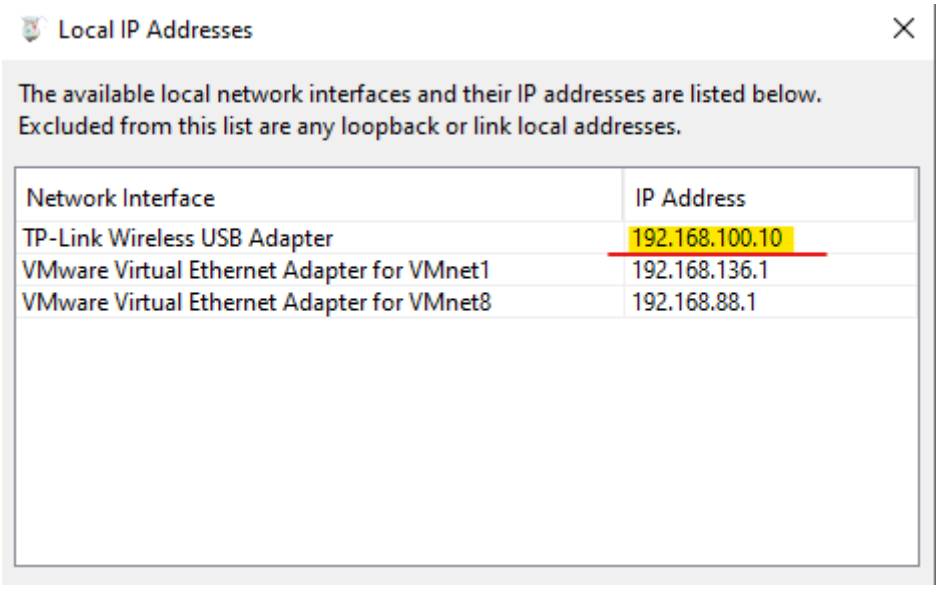
نحتاج ربطه في الجهاز الايفون الخاص بنا

١. نضغط على Help
٢. ثم نضغط على Local Ip Address

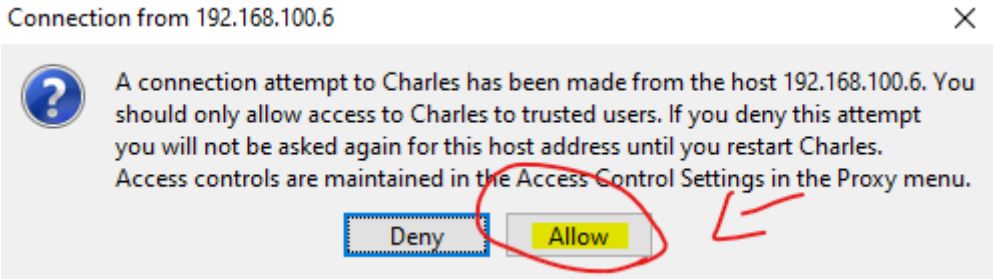


II7MAD99@GMAIL.COM 26 Oct 2021

الايبي نكتبه في الاعدادات الواي فأي - مثل الخطوات السابقة

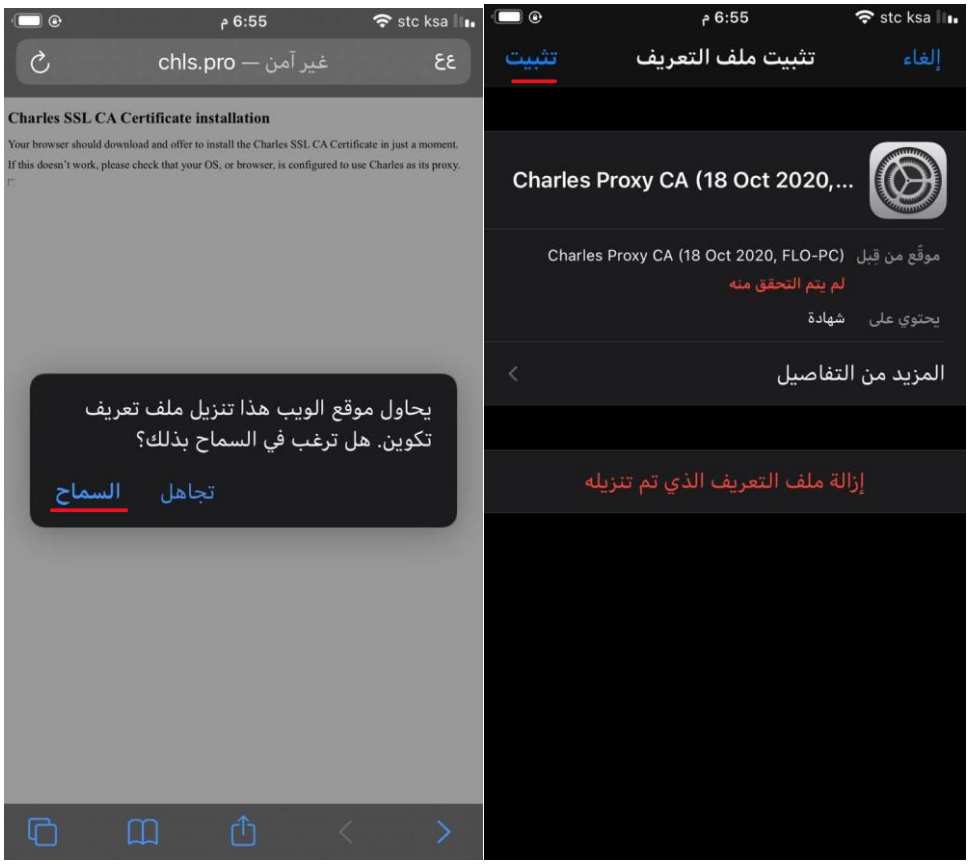


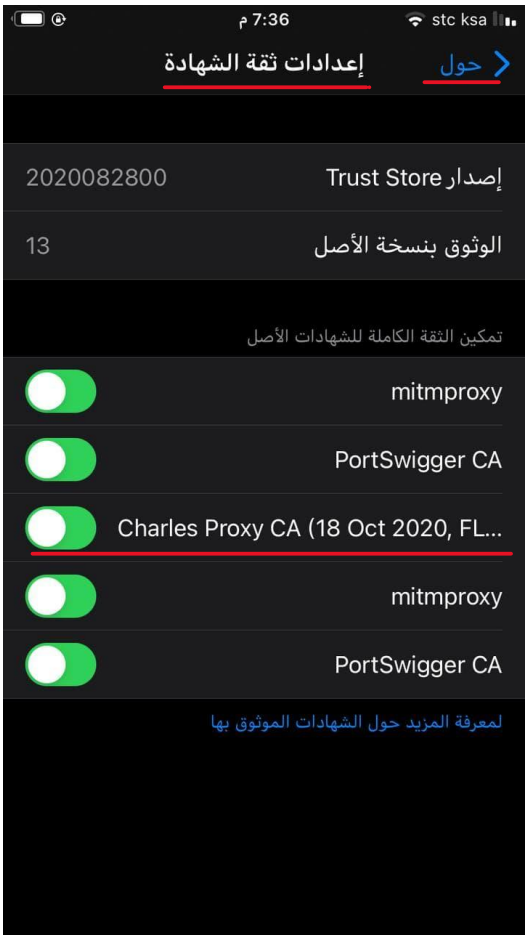
عند ربط الايبي في جهازك الايفون سوف تشاهد في البرنامج الرسالة تطلب منك الموافقة اضغط على Allow



ثم نذهب الي المتصفح ونكتب الرابط التالي: http://chls.pro/ssl

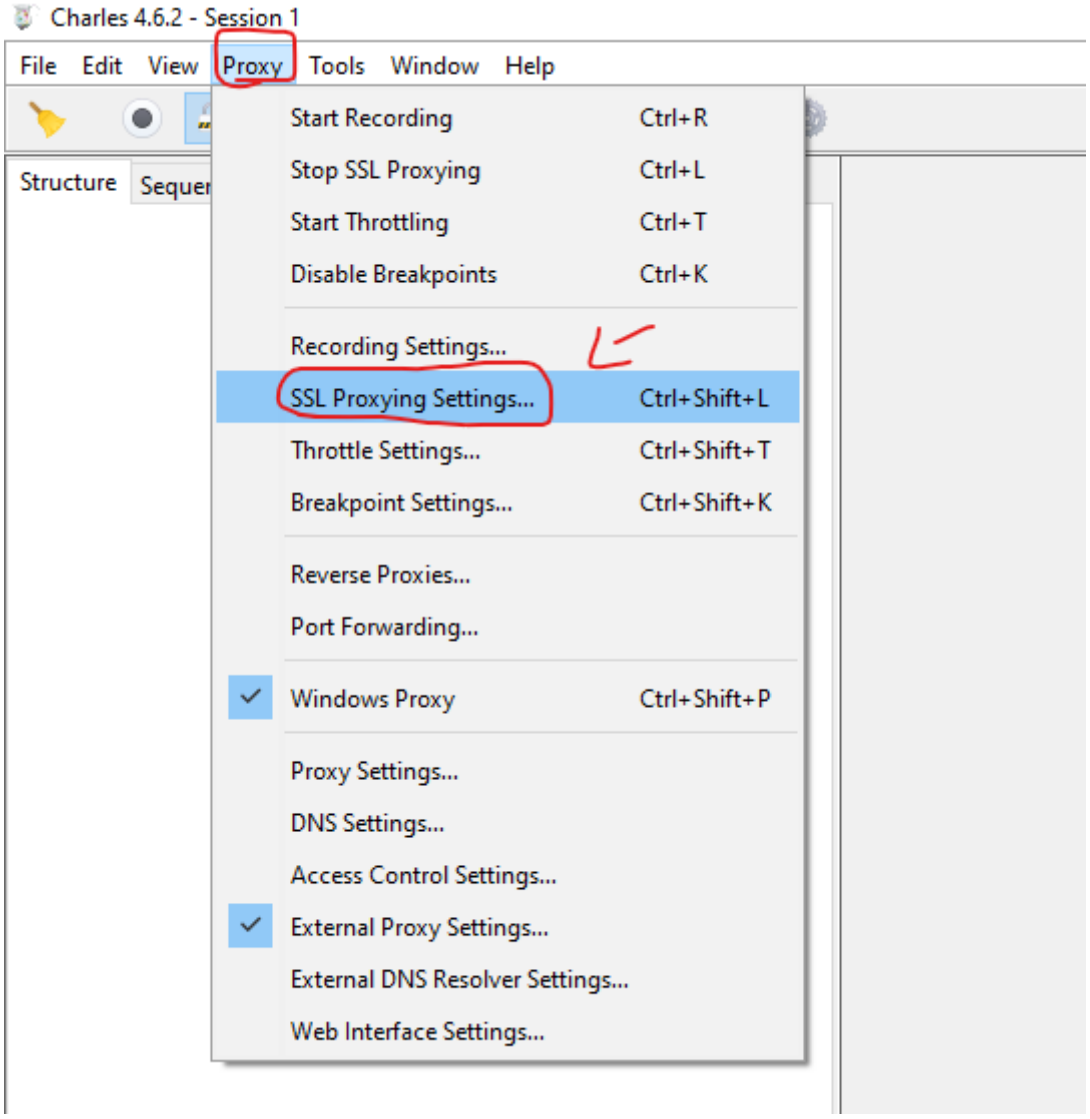
II7MAD99@GMAIL.COM 26 Oct 2021



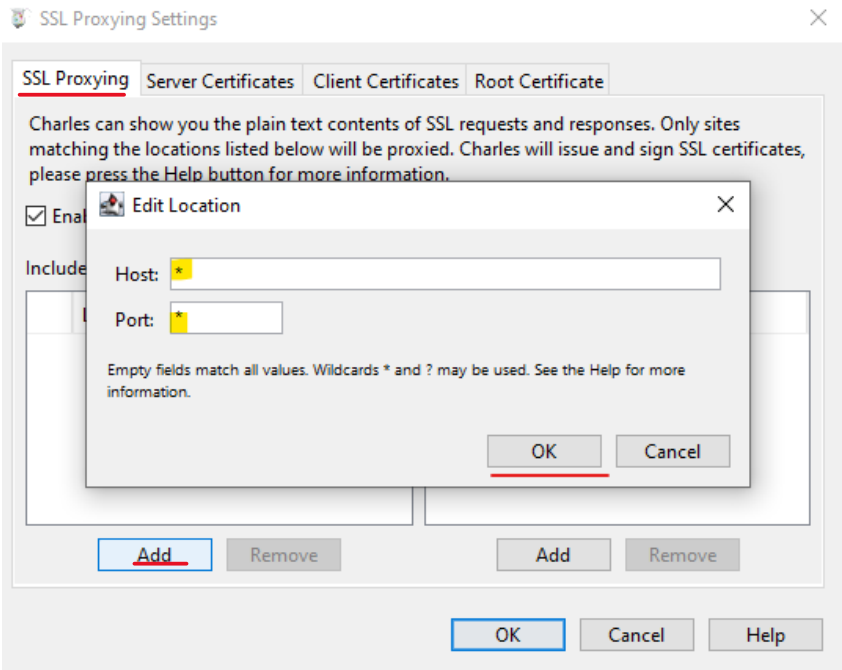


II7MAD99@GMAIL.COM 26 Oct 2021

ثم نتوجه الي **Proxy** في البرنامج ونضغط على ...**SSL Proxying Settings**



II7MAD99@GMAIL.COM 26 Oct 2021



الان جاهزين نفحص تطبيق Netflix ملاحظة رجع اصدار تطبيق الي 12.9.0

نتأكد من علامة الحمراء قيد التشغيل وجميع الخيارات

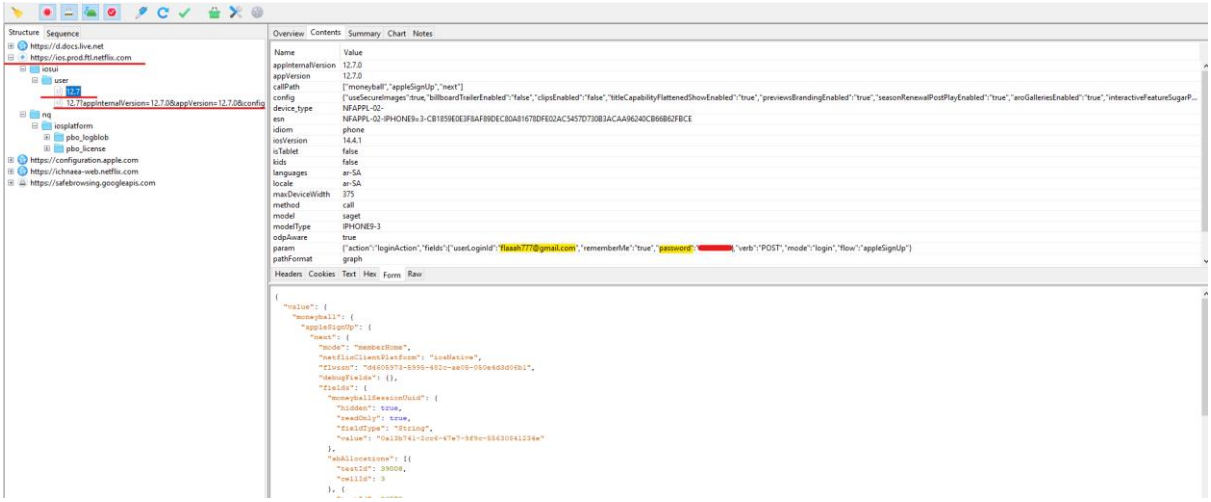
طلب تسجيل الدخول:

https://ios.prod.ftl.netflix.com/iosui/user/12.7

action":"loginAction","fields":{"userLoginId":"flaaah777@gmail.com","rememberM"}
{"e":"true","password":"######"},"verb":"POST","mode":"login","flow":"appleSignUp

تلاحظ في الداتا يوجد الاميل والباس الي طلبت أسجل دخول عليه في التطبيق

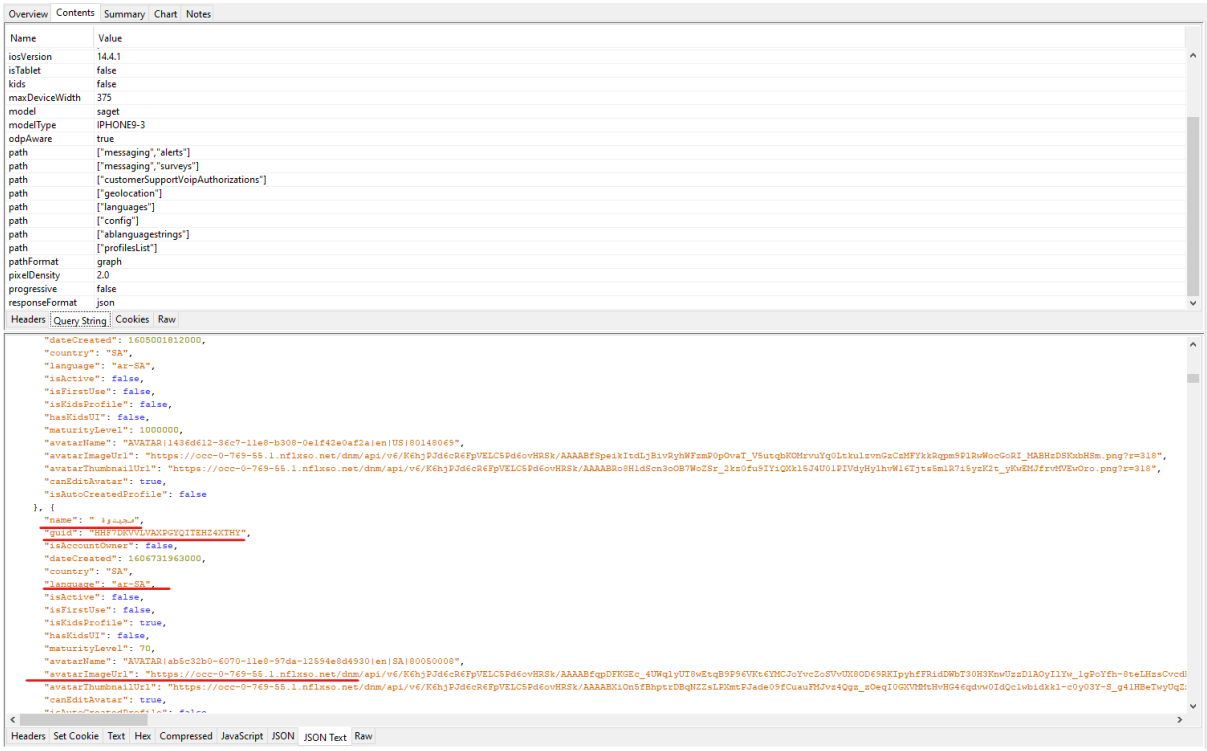
II7MAD99@GMAIL.COM 26 Oct 2021



داخل المسار يوجد مجلدين مجلد باسم 12.0 و appInternalVersion=12.7.0

- مجلد : 12.0 يوجد داخله طلب تسجيل الدخول
- مجلد appInternalVersion يوجد داخله رد السيرفر

appInternalVersion رد السيرفر:



تلاحظ تم تسجيل الدخول وجلب ملفات التعريف للحسابات وبياناتها

II7MAD99@GMAIL.COM 26 Oct 2021

ما هي أسرار تطبيقات الجوال؟

الأسرار هي أجزاء من المعلومات التي يجب ألا يعرفها طرف ثالث غير مشارك في الاتصال الأصلي. على معظم الأشكال الشائعة هي `symmetric keys` (a.k.a. shared keys)، `asymmetric keys (a.k.a.` secret/private keys)، `passwords` و`PINs`.

على سبيل المثال ، قد يرغب المطور في تشفير قاعدة البيانات المحلية لتطبيقه باستخدام SQLCipher لتنفيذ هذه العملية ، يحتاج التطبيق إلى توفير تسلسل أبجدي رقمي طويل `password` عادةً أو تريد مكتبة إرسال بعض الرسائل المشفرة إلى الواجهة الخلفية الخاصة بها وتستخدم أحد المعلمات لطريقة AES-256-GCM أو ChaCha20-Poly1305 أو يريد أحد التطبيقات إرسال رسالة موقعة إلى الخادم الخاص به باستخدام `shared keyprivate key` RSA

ما هي (عادة) ليست أسرارًا على تطبيقات الأجهزة المحمولة؟

ستمنح معظم أطر عمل الجهات الخارجية التي توفر خدمة سحابية للمطورين بعض بيانات الاعتماد لتسجيل الدخول على مواقع الويب الخاصة بهم وإدارة حساب المطور الخاص بهم. كجزء من وثائق التفويض، وتوفير هذه الخدمات أيضا ما يعرف عادة باسم `API key` و `API Token`. أو معظم هذه `API keys` ليست أسرارًا لأنها تعمل فقط كمعرفات. هذه الخدمات تريد أن تعرف *من* هو الوصول إلى واجهات برمجة التطبيقات وكانوا عادة ما يطلب منك إضافته إلى ملف التكوين التطبيق المحمول، (مثل `Info.plist`). *ولكن للتأكد فقط، يجب أن تؤكد مع مقدم الخدمة الخاص بك أنه* `API keys` *مسموح لهم أن يكونوا علنيين*

لماذا تعتبر تضمين الأسرار في تطبيقات الجوال فكرة سيئة؟

دعنا نعود إلى `secrets` الآن بعد أن أصبحنا على نفس الصفحة بشأن ما أسميه بيت القصيد من الأسرار هو. سبب عدم تضمين الأسرار في تطبيقات الجوال الخاصة بك

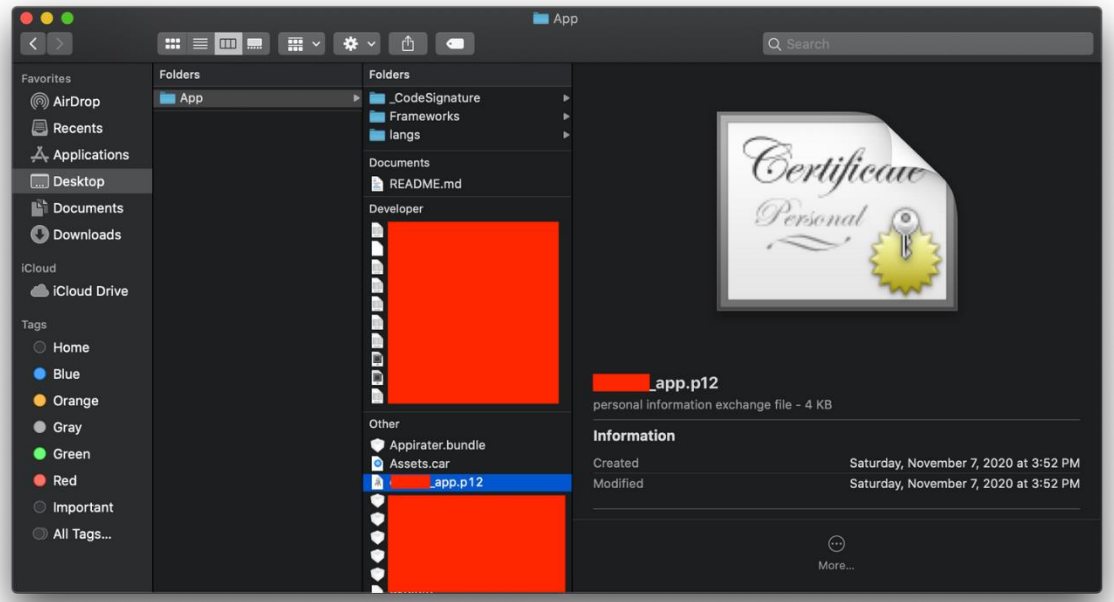
II7MAD99@GMAIL.COM 26 Oct 2021

حماية شيء ما، عادة ما يتم تخزين بيانات المستخدمين محليًا أو البيانات المرسلة إلى الواجهة الخلفية.

المشكلة الحقيقية هي أن أي سر مضمن في تطبيق جوال يمكن استرداده عن طريق الهندسة العكسية للتطبيق .يمكن تشويشها أو حتى تشفيرها (بسر آخر)، ولكن في نهاية اليوم، يحتاج التطبيق إلى استخدام السر ويمكن للمهاجمين استخدام وقت تشغيل التطبيق لإلغاء التعتيم أو فك تشفير السر .لكن هذا ليس ضروريًا بشكل عام، حيث إن معظم التطبيقات تحتوي فقط على الأسرار في نص عادي

دعنا نوضح النقطة بمثال من واقع الحياة

يحتوي هذا التطبيق على مفتاح خاص مضمن في الحزمة الخاصة به:



ولديها طريقة لتحميل هذا المفتاح السري RSA

loadPrivateKeyFromBundledP12: password: error:

II7MAD99@GMAIL.COM 26 Oct 2021


```
/* @class PPRSA */
-(bool)loadPrivateKeyFromBundledP12:(void *)arg2 password:(void *)arg3 error:(void * *)arg4 {
    r1 = _cmd;
    r31 = r31 - 0x80;
    var_40 = r26;
    stack[-72] = r25;
    var_30 = r24;
    stack[-56] = r23;
    var_20 = r22;
    stack[-40] = r21;
    var_10 = r20;
    stack[-24] = r19;
    saved_fp = r29;
    stack[-8] = r30;
    r21 = arg4;
    r23 = self;
    var_48 = **___stack_chk_guard;
    r19 = [arg2 retain];
    r20 = [arg3 retain];
    r0 = [NSBundle mainBundle];
    r0 = [r0 retain];
    r24 = r0;
    r0 = [r0 URLForResource:r19 withExtension:@"p12"];
    r29 = &saved_fp;
    r22 = [r0 retain];
    r0 = [r24 release];
    if (r22 == 0x0) goto loc_10009a20c;
```

p12 . شهادة مقفلة بكلمة مرور، ومع ذلك، يتم تضمين كلمة المرور في الملف الثنائي

```
sub_1001c0e40:
    adrp    x8, #0x10189d000                    ; 0x10189d4d0@PAGE, DATA XREF=-[_TtC7[redacted]TargetConfiguration A[redacted]NamePassword]
    add     x8, x8, #0x4d0                      ; 0x10189d4d0@PAGEOFF, "dM#A0CcK[redacted]"
    sub     x8, x8, #0x20                       ; 0x10189d4b0
    orr     x1, x8, #0x8000000000000000
    movz    x0, #0x1f
    movk    x0, #0xd000, lsl #48
    ret
  ; endp
```

كان هذا التطبيق يستخدم مفتاح RSA الخاص لطلب رمز مميز من الواجهة الخلفية والذي يمكن للتطبيق استخدامه بعد ذلك كرمز حامل لنظام مصادقة API الخاص بهم .أظن أن نيتهم كانت مصادقة طلبات واجهة برمجة التطبيقات بسلاسة ومنع الآخرين من الاستعلام عن واجهات برمجة التطبيقات الخاصة بهم لأنه "لا يوجد طلب أولي لواجهة برمجة التطبيقات موقّع"

تكمن المشكلة في أن أي شخص لديه المهارة الكافية لإجراء هندسة عكسية لتطبيقه، لديه حق الوصول إلى مفتاح RSA الخاص به، وبالتالي يمكنه تقديم طلبات API إلى نظامه الخلفي، متظاهرًا بأنه تطبيقه يؤثر هذا على أي نموذج (نماذج) معاملة أخرى تستند إلى نظام الثقة هذا.

وينطبق الشيء نفسه على قاعدة بيانات أو بيانات محلية مضمنة `password` او `symmetric encryption key` لحماية البيانات المرسلة إلى الواجهة

II7MAD99@GMAIL.COM 26 Oct 2021

سيتمكن المهاجم المتحمس من الوصول إلى أي أسرار تقوم بتضمينها في تطبيق الهاتف المحمول الخاص بك، وبالتالي سوف يعرض للخطر أي مخطط (مخططات) ثقة قمت بتصميمه بناءً على هذه الأسرار .من الأفضل عدم تضمين / ترميز الأسرار على تطبيقات الهاتف المحمول الخاصة بك .لن ينجزوا ما يحاول معظم المطورين استخدامه من أجله ويمنحهم فقط إحساسًا زائفًا بالأمان .وبالمثل كما هو الحال في "عالم الويب" حيث يُنصح بعدم الوثوق بأي مدخلات، لا تثق في طلبات واجهات برمجة التطبيقات الخاصة بتطبيق الجوال

المرجع: https://ivrodriguez.com/why-embedding-secrets-in-mobile-apps-is-not-a-good-idea

التحليل الديناميكي

باستخدام بعض المعلومات التي تم جمعها من التحليل الثابت، يمكنك البدء في تنفيذ بعض القرصنة الديناميكية

- استخدم أداة التحليل الديناميكي لفحص سلوك التطبيق في وقت التشغيل:
  استخدم cycript ، frida أو حتى gdb
- إذا وجدت أي فئات / طرق
  بها developer ، development ، test ، fake ، funtio debug nality، فحاول تمكينها عن طريق استدعاء هذه الطرق .على سبيل المثال، كان هناك تطبيق واحد يحتوي على فئة
  تسمى InternalSettingsViewController ، عند تقديمه ، ستعرض وحدة التحكم هذه الكثير من معلومات تصحيح الأخطاء

- إذا كان التطبيق لا يتم تحميل أو تحطمها عند إطلاق immediately ، في محاولة للبحث في تفريغ فئة (أو في المجمع الخاص بك) لطرق
  مثل isJailbroken ، jailbreak ، rooted ، لأن هناك احتمالات لديهم الكشف عن الهروب من السجن .معظم هذه المكتشفة يمكن تجاوزه مع السيديا
  مثل xCon ، NoSub أو tsProtector
- بعد تشغيل التطبيق وربما التسجيل أو اللعب معه لفترة من الوقت، تحقق من iOS Keychain للحصول على البيانات التي تم إنشاؤها من التطبيق يقوم

II7MAD99@GMAIL.COM 26 Oct 2021

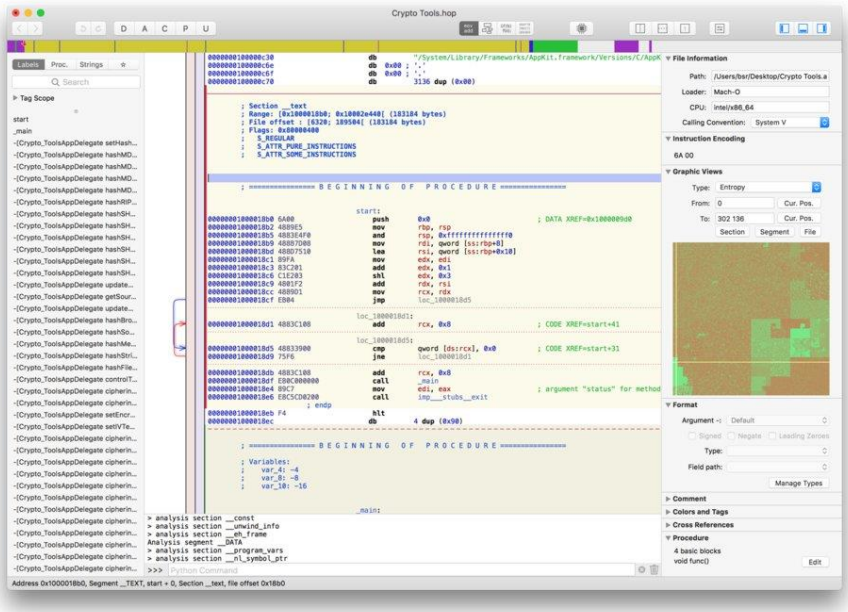
بعض المطورين بتخزين بيانات اعتماد AWS / GCP هناك:
استخدمها Keychain-Dumper لتفريغ عناصر سلسلة المفاتيح.

- أيضًا، بعد استخدام التطبيق لفترة من الوقت، تحقق من UserDefaults الملف، وهو plist. ملف تكوين يستخدمه بعض المطورين لتخزين معلومات حساسة: يوجد الملف في /private/var/mobile/Containers/Data/Application/{uuid}/Library/Preferences ويُعرف باسم معرف حزمة التطبيق .plist.
- تجاوز حركة مرور TLS في App Store ، وافتحBurp ، وحدد Proxy ، ثم قم Options بالتمرير لأسفل TLS Pass Through وأضف:
  - ^.*?apple\..*$
  - ^.*?icloud\..*$
  - ^.*?mzstatic\..*$

التحليل الساكن

بعد تنزيل التطبيق وفك تشفيره من أداة frida-ios-dump ، قم بتحميله على برامج التفكيك على سبيل المثال ، برنامج hopper على الحاسوب

https://www.hopperapp.com



II7MAD99@GMAIL.COM 26 Oct 2021

العديد من مفاتيح تشفير الرموز الثابتة للمطورين أو بيانات اعتماد العميل على تطبيقات iOS حدد Strings علامة التبويب وابحث عن هذه المصطلحات secret ، crypt ، private ، token.

- تستخدم العديد من التطبيقات أنظمة خلفية خارجية ، لذلك تحتاج التطبيقات إلى بعض بيانات الاعتماد أو ملفات التكوين .أحيانا المطورين كشف وثائق التفويض أو مفاتيح خاصة في هذه الملفات: في بحث حزمة من التطبيق لكافة .plist ، .json أو .conf الملفات التي يمكن العثور عليها .المشتركة AirshipConfig.plist ، GoogleService-Info.plist وبالتأكيد التطبيق الخاص Info.plist

- هناك الكثير من التطبيقات التي تحتوي على فئات تطوير / تصحيح أخطاء أو طرق تعرض معلومات أكثر مما يجب أن يراه المستخدم العادي أو يضع التطبيق في وضع تصحيح الأخطاء الذي سيساعد في جمع معلومات إضافية:
حدد Procedures علامة التبويب وابحث عن هذه المصطلحات develop ، debug ، fake ، test.
- في كثير من الأحيان ، ينسى المطورون إزالة بيانات / ملفات الاختبار من مشروع XCode وينتهي بهم الأمر مجمعة داخل التطبيق: ابحث في دليل حزمة التطبيق عن الملفات التي ليست صورًا أو .storyboardc / .xib ، على سبيل المثال .json.
- ابحث في الملف الثنائي عن مفاتيح التشفير المشفرة باستخدام strings الأمر:
  - سلاسل أبجدية رقمية تتكون من ٦٤ حرفًا:

```
strings <binary> | grep -E '^[[:alnum:]]{64,64}$'
```

  - UUIDs:

```
strings <binary> | grep -E '^[-[:alnum:]]{36,36}$'
```

- افحص الملفات التي يخزنها التطبيق ، بما في ذلك البيانات من مكتبات الجهات الخارجية التي تم استيرادها بواسطة التطبيق الرئيسي SSH : في جهازك وقم بتغيير الدلائل إلى .{/private/var/mobile/Containers/Data/Application/{UUID
- تفريغ الطبقات والأساليب والمتغيرات من التطبيق class-dump <binary> > dump.txt
- يستخدم كل تطبيق جوال تقريبًا مكتبة جهة خارجية واحدة على الأقل .ابحث في مكتبات الجهات الخارجية هذه وتحقق من إصداراتها ، فالكثير منها مفتوح المصدر ويمكنك البحث في المستودعات العامة الخاصة issues بها والتحقق مما إذا كان الإصدار الحالي من المكتبة يتأثر / لا يتأثر .جميع المكتبات موجودة داخل Frameworks/ المجلد في حزمة التطبيق

II7MAD99@GMAIL.COM 26 Oct 2021

أهم 4 عيوب أمنية لتطبيقات الهاتف المحمول الأكثر شيوعًا

سواء كنت مبتذلًا وتتطلع إلى اكتساب بعض الخبرة في اختراق الأجهزة المحمولة أو مطورًا يهدف إلى إنشاء تطبيقات آمنة ، فإن التعرف على بعض أخطاء الأمان الشائعة التي يرتكبها المطورون سوف يخدمك جيدًا .لقد أدرجت ولخصت هنا الأنواع الاربعة الأكثر شيوعًا من عيوب أمان تطبيقات الأجهزة المحمولة التي رأيتها في العالم الحقيقي سأصف كل العيوب وتأثيرها والأسباب المحتملة وراء ظهورها بشكل متكرر بالطبع ، هذه القائمة تستند فقط إلى تجربتي الخاصة ولا تدعمها أي إحصاءات رسمية

1 #عيوب / SSL / انسان في الوسط

يحتوي iOS على رمز معالجة الشهادة ، ولكن عندما يقرر مطورو التطبيقات كتابة التنفيذ الخاص بهم ، فهناك فرصة جيدة لارتكابهم خطأ .إذا لم يتحقق التطبيق من صحة سلاسل الشهادات وتوقيعاتها بشكل صحيح ، فقد يخدع المهاجم التطبيق لقبول شهادة تنتحل صفة خادم التطبيق

يمكن أن تؤدي عيوب معالجة الشهادات إلى وجود ثغرات أمنية تسمح للمهاجمين بالتنصت على الاتصالات أو تعديلها .تحدث أخطاء SSL هذه عادةً عندما يقرر المطورون تنفيذ رمز معالجة الشهادة الخاص بهم ، ربما بسبب وجود بعض الوظائف المفقودة في المكتبات الأصلية التي يريدون استخدامها .في أوقات أخرى ، يمكن أن تحدث عندما يستخدم المطورون المزيد من إعدادات أمان الشبكة المتراخية أثناء مرحلتي التطوير والاختبار ونسيان تغيير هذه الإعدادات مرة أخرى في تطبيق الإنتاج

2 #الشركات الضعيفة التي عفا عليها الزمن

ربما قد تكون شاهدت شخص ابلغ شركة تطبيق في تصحيح ثغرة أمنية يحدث ذلك غالبًا لكل من تطبيقات iOS و Android بعد استلام البلاغ سيحاول مالكو هذه الشركات عادةً تنبيه المطورين وإبلاغهم بتصحيح على الفور - لكن هؤلاء المطورين لا ينتبهون دائمًا او ليس لديهم خبره الكافية

بتصحيح الخطاء او اغلاق الثغرة الأمنية

3 #مرجع كائن مباشر غير آمن (IDOR)

بينما يمكنك القول أن IDORs ليست عيبًا تقنيًا في تطبيق الهاتف المحمول نفسه ، فغالبًا ما يمكن العثور عليها في REST API للتطبيق .بالنسبة لأولئك غير المألوفين ، يقدم PortSwigger هذا التعريف:

II7MAD99@GMAIL.COM 26 Oct 2021

مراجع الكائنات المباشرة غير الآمنة (IDOR) هي نوع من الثغرات الأمنية للتحكم في الوصول التي تنشأ عندما يستخدم أحد التطبيقات المدخلات التي يوفرها المستخدم للوصول إلى الكائنات مباشرة

https://portswigger.net/web-security/access-control/idor

إليك مثال أساسي: لنفترض أننا قمنا بتسجيل الدخول إلى أحد تطبيقات المراسلة واعترضنا طلبًا لنقطة النهاية هذه عندما نفتح صندوق الوارد الخاص بنا:

```
http https://xxxxx.com/messages/inbox/latest?id=1948992
```

يمكننا أن نستنتج أن هذه المكالمة تجلب أحدث رسائلنا وأن "١٩٤٨٩٩٢" هو معرف المستخدم الخاص بنا .إذن ماذا يحدث إذا قمنا بتغيير معلمة "id" إلى معرف مستخدم مختلف ؟

```
https://xxxxx.com/messages/inbox/latest?id=37173925
```

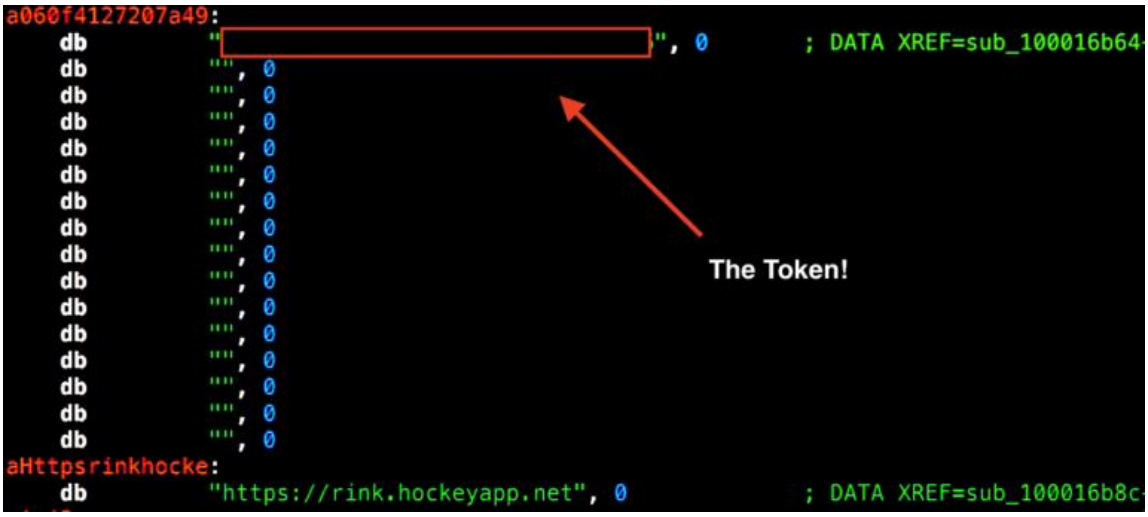
قد يعرض التطبيق غير المعرض للخطر خطأً لأننا غير مصرح لنا بقراءة البريد الوارد لهذا المستخدم .ولكن عند وجود IDOR ، ستنجح المكالمة وسنكون قادرين على قراءة رسائل الضحية !

من واقع خبرتي ، فإن IDORs في واجهات برمجة التطبيقات للجوال شائعة بنفس القدر ، إن لم تكن أكثر شيوعًا مما هي عليه

II7MAD99@GMAIL.COM 26 Oct 2021

4 #أسرار مشفرة

ربما رأى معظمكم هذا قادمًا .اعتمادًا على ما تم الكشف عنه ، يمكن أن يتراوح التأثير في أي مكان من إزعاج خفيف إلى كارثة كاملة .تتضمن بعض الأسرار التي يتم تسريبها بشكل شائع بيانات اعتم AWSومفاتيح Google API وعلامات API للشبكة الاجتماعية والمفاتيح الخاصة RSA



تم العثور على الأسرار المسربة في كل مكان تقريبًا ، في تطبيقات الويب ، وأجهزة إنترنت الأشياء ، ومستودعات جيثب ، والمزيد ولكن مرارًا وتكرارًا ، يبدو أن بعض أسوأ عمليات الكشف تنشأ من تطبيقات الأجهزة المحمولة هناك العديد من التفسيرات المعقولة لهذا الاتجاه

أعتقد أن السبب الأساسي بسيط: كثير من الناس لا يدركون أن تطبيقات الأجهزة المحمولة يمكن عكسها يعرف معظم مطوري الويب أن الكود الذي يكتبونه سيكون متاحًا للجمهور ويتم تذكيرهم باستمرار بمراعاة ذلك ربما يعتقد بعض المطورين أن نظام تشغيل الهاتف المحمول نفسه يوفر بعض الحماية - وهذا صحيح - لكن هذا لا يكفي لمنع شخص ما من الاطلاع على العناصر الداخلية لتطبيقهم في أوقات أخرى

المرجع :

https://www.allysonomalley.com/2020/06/23/the-top-5-most-common-mobile-app-security-flaws

فحص تطبيقات الايفون من الايفون

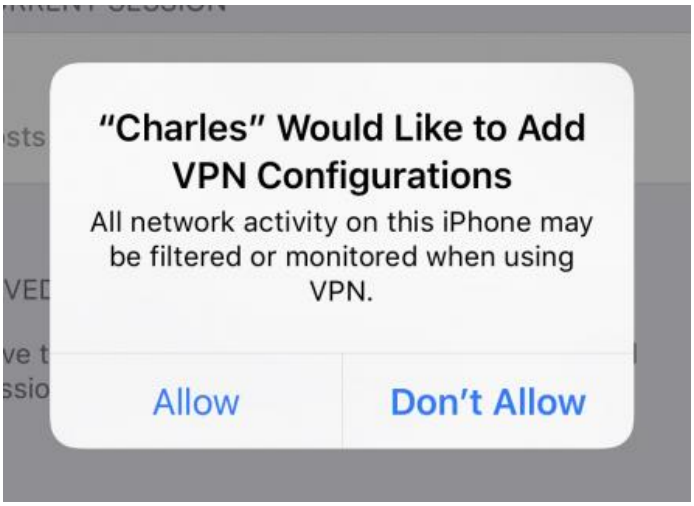
ستفحص من تطبيق Charles Proxy لنظام iOS !

افتح App Store على جهاز iOS الخاص بك وابحث عن Charles Proxy لسوء الحظ ، لا يوجد إصدار مجاني من تطبيق iOS ، لذا سيتعين عليك شرائه إذا كنت ترغب في متابعة هذا القسم

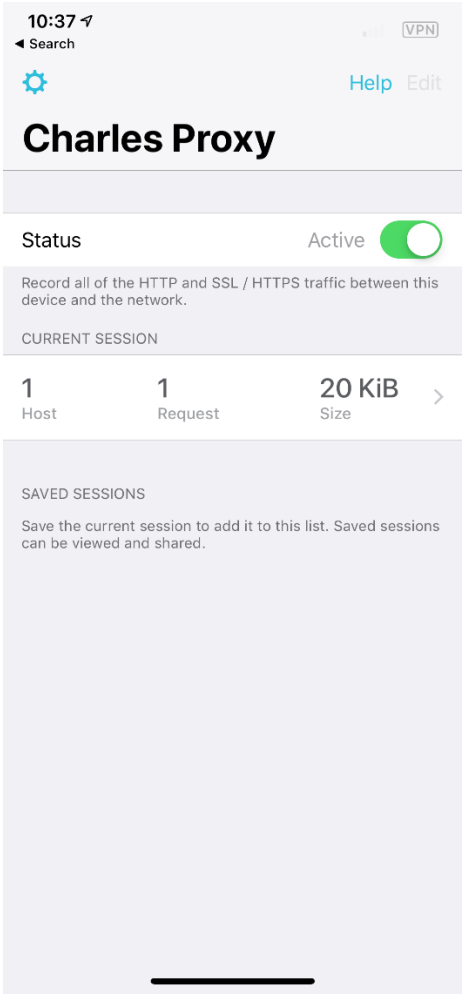
II7MAD99@GMAIL.COM 26 Oct 2021

قم بتثبيت التطبيق على جهازك وافتحه تظهر الشاشة الأولية أن الوكيل غير نشط هناك مفتاح تبديل ونظرة عامة على بعض الإحصائيات الرئيسية لأي جلسة قيد التشغيل قم بتبديل مفتاح الحالة قيد التشغيل

بمجرد مطالبتك بالإذن لتثبيت تكوينات VPN ، انقر فوق السماح

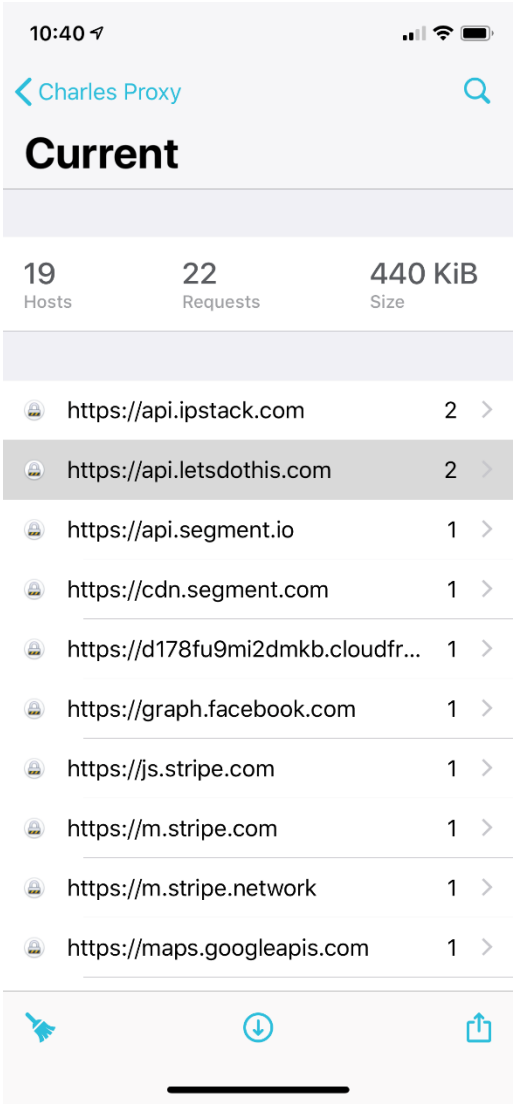


II7MAD99@GMAIL.COM 26 Oct 2021



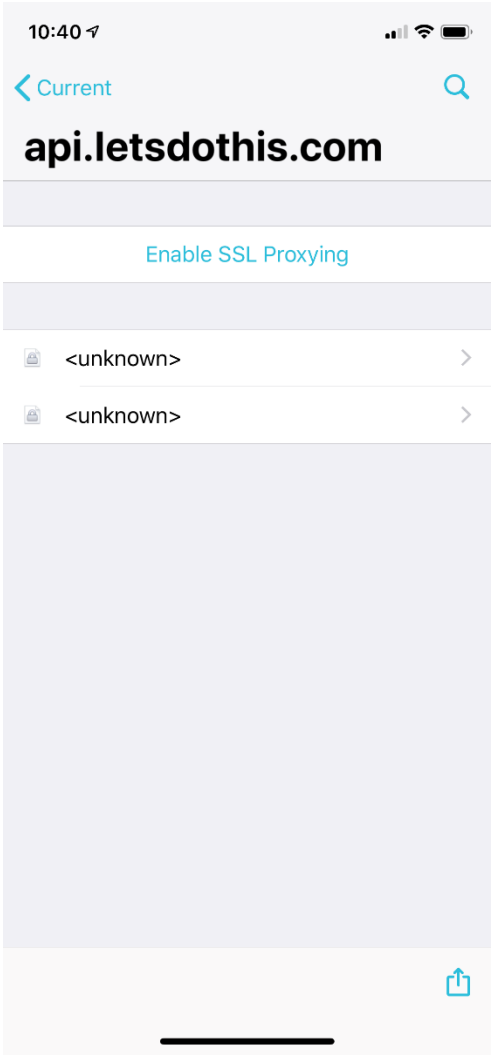
ستتغير الحالة إلى نشط

II7MAD99@GMAIL.COM 26 Oct 2021



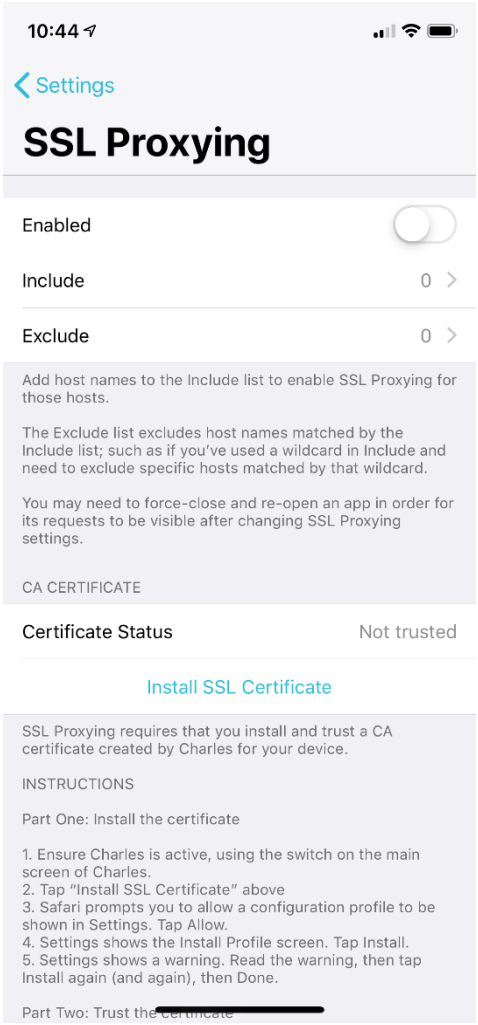
انقر فوق سهم مؤشر الكشف عن الجلسة الحالية ، وسينتقل التطبيق إلى طريقة عرض مماثلة للجزء العلوي في تطبيق سطح المكتب .إذا كنت لا ترى أي طلبات ، فانتقل إلى Safari وقم بتحميل صفحة ويب

II7MAD99@GMAIL.COM 26 Oct 2021



انقر فوق أي من الطلبات الفردية وستنتقل إلى عرض تفصيلي لهذا الطلب .كما هو الحال مع تطبيق سطح المكتب ، لا تزال أي حركة مرور مشفرة SLS / TLS غامضة

II7MAD99@GMAIL.COM 26 Oct 2021



حان الوقت لإصلاح ذلك :

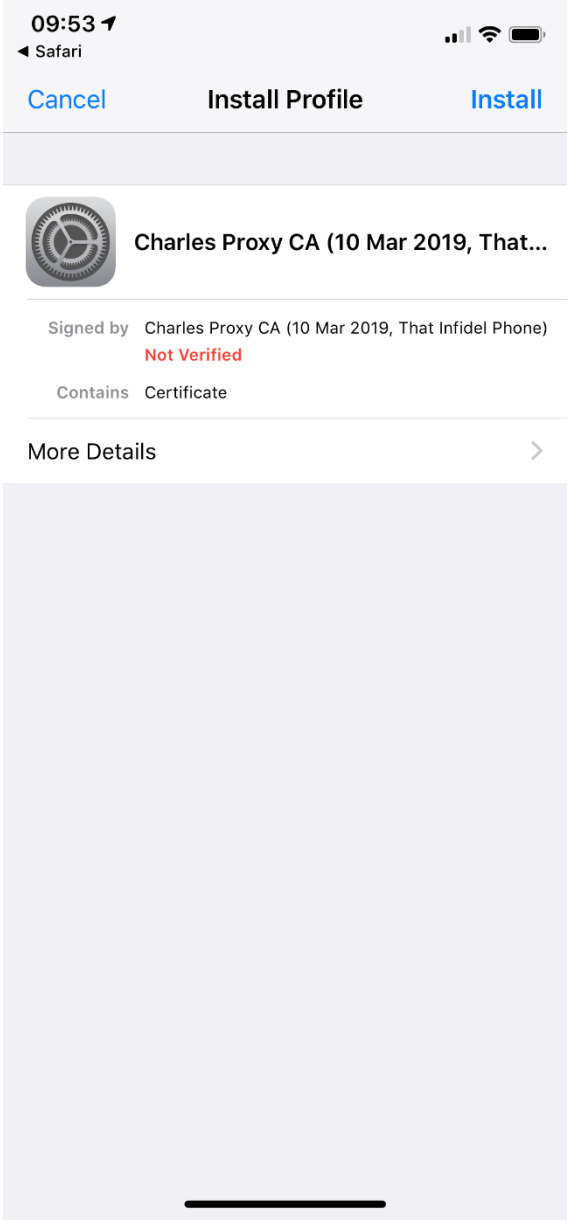
تثبيت شهادة تشارلز

لا يزال داخل تطبيق Charles Proxy ، انتقل مرة أخرى إلى الشاشة الأولية من خلال النقر على السهم الخلفي في أعلى يسار الشاشة مرتين .مع استمرار نشاط الوكيل ، انقر فوق ترس الإعدادات أعلى يسار الشاشة .حدد SSL Proxyin

الآن ، في الجزء السفلي من هذه الشاشة ، ستجد إرشادات مفصلة حول تثبيت شهادة Charles Proxy CA والثقة بها أولاً ، قم بتثبيت الشهادة باستخدام الزر الموجود في التطبيق سيتحول جهازك إلى تطبيق Safari ويطلب الإذن لتثبيت الملف الشخصي

ملاحظة :إذا كان لديك Apple Watch مقترنة بجهازك ، فسوف يسألك عما إذا كنت تريد تثبيت ملف التعريف على الجهاز أو الساعة .اختر . iPhone

II7MAD99@GMAIL.COM 26 Oct 2021



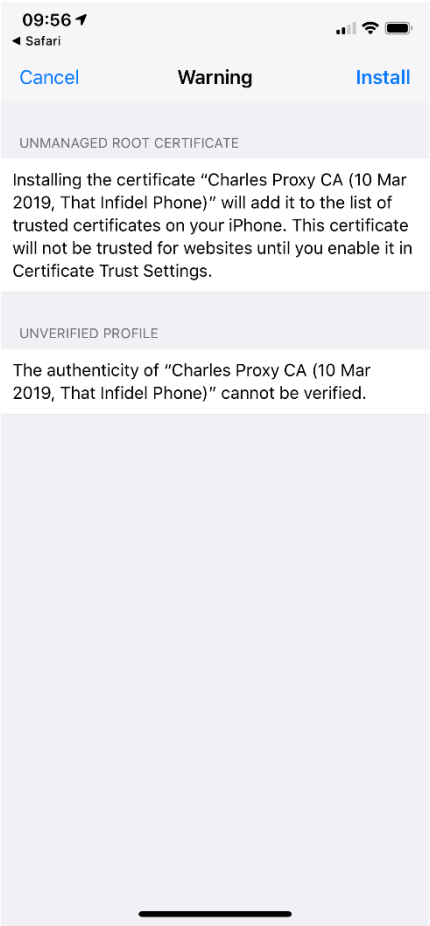
بمجرد تثبيت ملف التعريف ، افتح تطبيق الإعدادات سترى خيار تنزيل ملف تعريف جديد اضغط عليه واختر خيار التثبيت في الزاوية العلوية اليمنى

Install

ستتم مطالبتك بإدخال رمز المرور الخاص بجهازك ، إذا كان لديك واحد ، متبوعًا بشاشة تأكيد تحذرك من أن هذه الشهادة لم يتم التحقق منها .انقر فوق تثبيت مرة أخرى .أخيرًا ، ستظهر شاشة إجراء من أسفل الشاشة مع تأكيد نهائي تريد Apple حقًا التأكد من أنك تريد تثبيت هذا

مرة أخرى ، لا تقم بتثبيت أي شهادة عشوائية ، وإلا يمكنك تكوين أمان الشبكة!

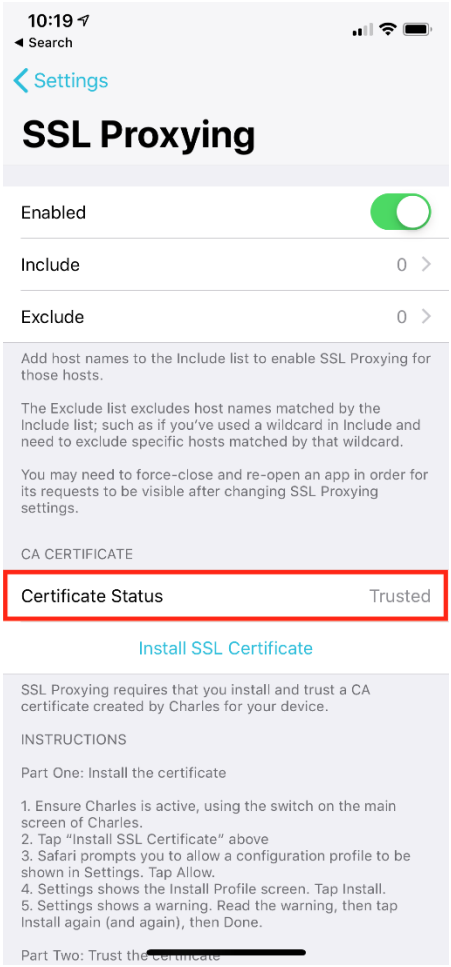
II7MAD99@GMAIL.COM 26 Oct 2021



عليك أن تثق بهذه الشهادة .لا يزال في تطبيق الإعدادات ، انتقل إلى عام حول ▸ شهادة الثقة إعدادات .ابحث عن شهادة Charles Proxy وقم بتبديل المفتاح إلى وضع التشغيل سيظهر مربع حوار تحذير .حدد متابعة

عد إلى تطبيق Charles Proxy وستظهر حالة الشهادة
الآن موثوقة بدّل مفتاح Enabled في الجزء العلوي من الشاشة إلى وضع التشغيل

II7MAD99@GMAIL.COM 26 Oct 2021

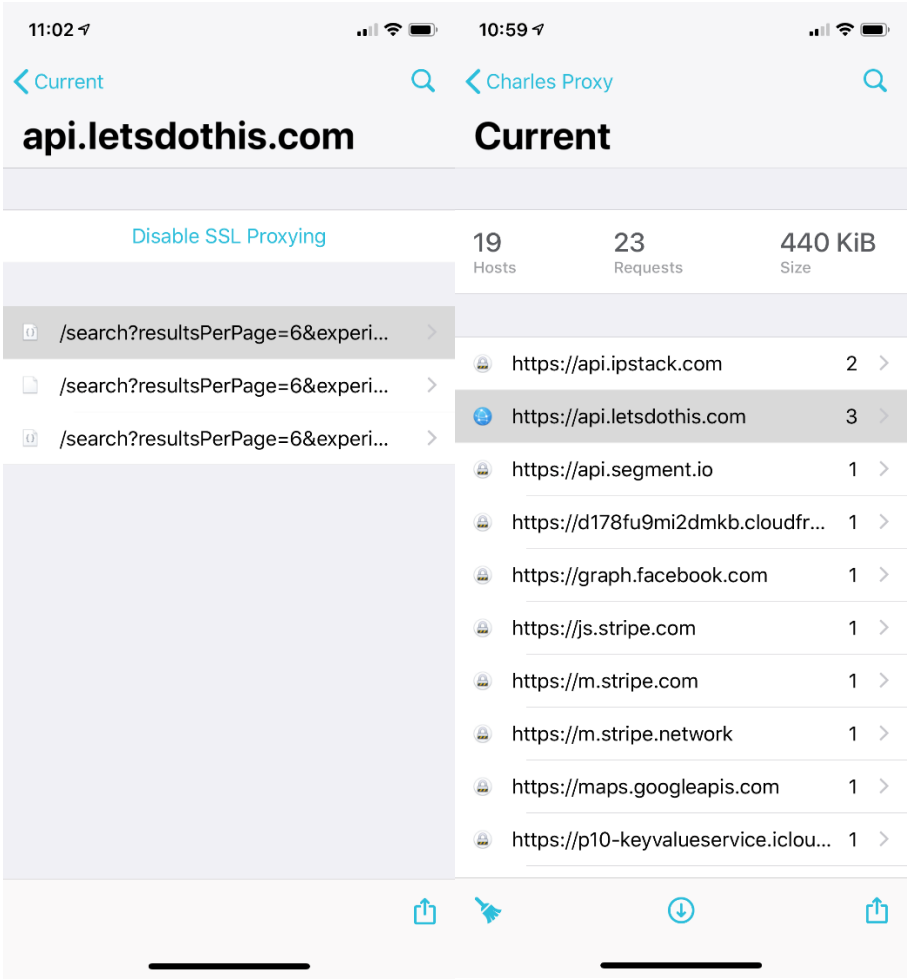


في Charles ، انتقل مرة أخرى إلى صفحة الإعدادات الرئيسية واحفظ التغييرات افتح الجلسة الحالية وامسح كل حركة المرور باستخدام أيقونة المكنسة في الركن الأيسر السفلي من الشاشة .انتقل إلى Safari وأعد تحميل صفحة ويب .ثم انتقل مرة أخرى إلى .Charles Proxy انقر فوق أحد الطلبات

وانقر فوق تمكين SSL Proxying

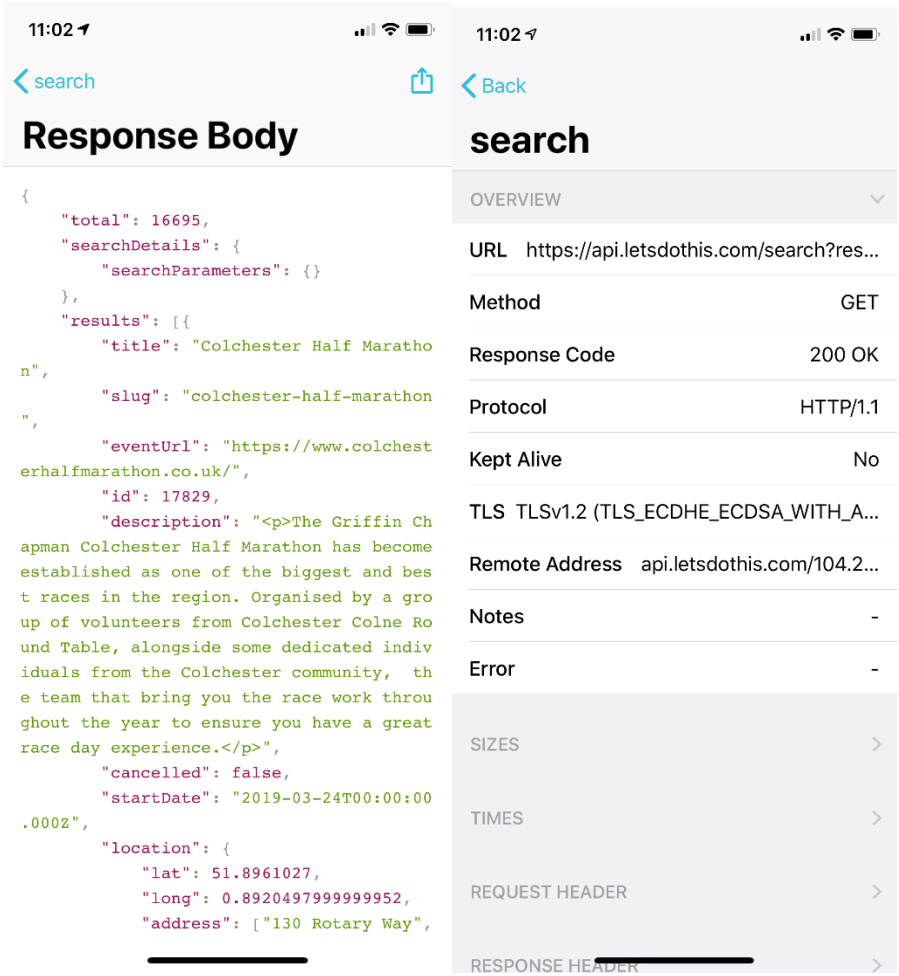
ارجع إلى الجلسة الحالية وامسح الجلسة مرة أخرى .أعد فتح Safari وأعد تحميل الصفحة في المرة الأخيرة .الآن ، إذا انتقلت مرة أخرى إلى Charles Proxy ، فسيكون لعنوان URL الذي قمت بتمكين وكلاء SSL له رمز شبكة أزرق بدلاً من رمز قفل

II7MAD99@GMAIL.COM 26 Oct 2021



أولاً ، انقر فوق عنوان URL لمعرفة التفاصيل الكاملة لكل طلب
بعد ذلك ، اضغط على طلب للحصول على مزيد من التفاصيل

II7MAD99@GMAIL.COM 26 Oct 2021



بعد ذلك ، انقر فوق " عرض النص "لعرض نص الاستجابة بالكامل ..

استخدم هذا المثال Safari، ولكن العملية التالية ستعمل عند فتح أي تطبيق على جهازك ، بما في ذلك التطبيق الخاص بك ، عندما تريد تصحيح أخطاء شبكة تطبيقك

بعد ذلك ، انقر مرة أخرى على صفحة الطلب وقم بتعطيل وكلاء SSL انقر مرة أخرى على العرض الأولي واضبط حالة Charles Proxy على Inactive لإيقاف إنشاء وكلاء لحركة المرور

مرجع :

https://www.raywenderlich.com/21931256-charles-proxy-tutorial-for-ios

II7MAD99@GMAIL.COM 26 Oct 2021

تحليل تطبيقات الايفون بواسطة الطب الشرعي

لذلك ، قبل أن نبدأ ، نحتاج إلى تلبية بعض المتطلبات

- وجود جلبريك
- تحميل أداة **openssh** من السيديا
- نحتاج أيضًا إلى **iProxy** ، الموجود في حزمة أدوات: **libusbmuxd**

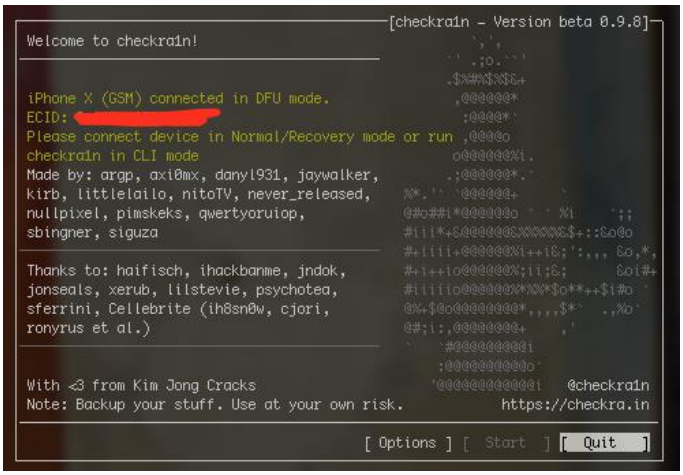
```
sudo apt install libusbmuxd-tools
```

يمكن جلب *checkra1n* من المستودع الرسمي تم اختباره على: Debian / Linux
ملاحظة - تستطيع تطبيق اشرح في أي نوع من انواع الجلبريك

```
echo "deb https://assets.checkra.in/debian /" | sudo tee -a /etc/apt/sources.list

sudo apt-key adv --fetch-keys https://assets.checkra.in/debian/archive.key

sudo apt update

sudo apt install checkra1n
```

تشغيل الجلبريك بعد تنزيله اكتب :

```
sudo checkra1n
```



II7MAD99@GMAIL.COM 26 Oct 2021

بمجرد بدء تشغيل الجهاز ، يمكنك تشغيل iproxy للسماح لك بدخول SSH إلى جهاز iOS عبر: USB

```
$ iproxy 4242 22
```

من الممكن الآن الوصول إلى الجهاز عبر SSH كلمة مرور الجذر هي: alpine
كلمة المرور الافتراضيه إذا لم تغيرها سابقا

```
$ ssh root@127.0.0.1 -p 4242
```

ضع الايبي الخاص في جهازك الايفون من الاعدادات الواي فاي في مكان 127.0.0.1

إجراء الاستحواذ

من أجل إجراء اكتساب "تقسيم إلى صورة" ، يمكنك استخدام: DD

```
ssh root@127.0.0.1 -p 4242 dd if=/dev/rdisk0s1s1 bs=4k | dd of=system.dd
```

علاوة على ذلك ، يمكنك أيضًا الحصول على بيانات المستخدم باستخدام: tar

```
$ ssh root@127.0.0.1 -p 4242 'tar -cf - /private/var/' > private-var.tar
```

تثبيت :

```
git clone https://github.com/abrignoni/iLEAPP

sudo apt-get install python3-tk

cd iLEAPP

pip install -r requirements.txt
```

II7MAD99@GMAIL.COM 26 Oct 2021

طريقة الاستعمال :

```
abrignoni@Alexiss-MBP iLEAPP % python3 ileapp.py -h
usage: ileapp.py [-h] -t {fs,tar,zip,gz,itunes} -o OUTPUT_PATH -i INPUT_PATH

iLEAPP: iOS Logs, Events, and Plists Parser.

optional arguments:
  -h, --help            show this help message and exit
  -t {fs,tar,zip,gz,itunes}
                        Input type (fs = extracted to file system folder)
  -o OUTPUT_PATH, --output_path OUTPUT_PATH
                        Output folder path
  -i INPUT_PATH, --input_path INPUT_PATH
                        Path to input file/folder
```

```
python ileapp.py -t <zip | tar | fs | gz | itunes> -i
<path_to_extraction> -o <path_for_report_output>
```

للتثبيت والاستخدام على **macOS** ، يرجى **الرجوع** إلى هذا الفيديو المفيد بواسطة : **13cubed**

https://www.youtube.com/watch?v=fEYV5vVAdu4

مراجع

١. https://github.com/abrignoni/iLEAPP
٢. https://github.com/abrignoni/iLEAPP/releases

II7MAD99@GMAIL.COM 26 Oct 2021

كيفية التحقق من برنامج التجسس على جهاز iPhone الخاص بك ؟

زعم تقرير حديث صادر عن مشروع Pegasus ، وهو اتحاد من المنظمات غير الهادفة للربح والعديد من الصحفيين ، أنه اكتشف تسربًا لـ ٥٠,٠٠٠ رقم هاتف من المحتمل أن يكون ملكًا لمستخدمين قد يكونون ضحايا لبرامج التجسس Pegasus، التي طورتها شركة التكنولوجيا الإسرائيلية. NSO
أصدرت منظمة العفو الدولية ، وهي جزء من المجموعة ، أداة للتحقق مما إذا كان هاتفك قد تأثر ، تسمى *مجموعة أدوات التحقق من الهاتف المحمول* ، أو MVT
في هذا القسم ، سنبحث عن خطوات لتحليل iPhone باستخدام جهاز Linux

أداة MVT يمكن تركيبها بسهولة من جيثب مستودع:

```
git clone https://github.com/mvt-project/mvt.git
cd mvt
pip3 install
```

ومع ذلك ، تحتاج أيضًا إلى حل بعض التبعيات:

```
sudo apt install python3 python3-pip libusb-1.0-0
```

من أجل تحليل جهاز iOS ، نحتاج إلى جمع البيانات الوصفية من نظام الملفات: بعد ذلك ، يمكن تحليل هذه البيانات باستخدام MVT

تتوفر حاليًا منهجيتان للاكتساب : "النسخ الاحتياطي" و "تفريغ نظام الملفات"

أكثر بساطة ومتوفر على جميع الأجهزة ، وكذلك الأجهزة " *غير مكسورة الحماية* ."
بينما لا توفر النسخ الاحتياطية سوى مجموعة فرعية من الملفات المخزنة على الجهاز ، فقد يكون ذلك كافياً في كثير من الحالات لاكتشاف بعض القطع الأثرية المشبوهة."Pegasus"
في نظام Linux ، يمكنك إجراء نسخ احتياطي باستخدام libimobiledevice ، والذي يمكن تثبيته على Debian , Linux باستخدام الأوامر التالية:

```
sudo apt install usbmuxd libimobiledevice6 libimobiledevice-utils ideviceinstaller
```

II7MAD99@GMAIL.COM 26 Oct 2021

ثم يمكنك توصيل iPhone بمنفذ USB على محطة العمل الجنائية الخاصة بك وقبول طلب الاقتران على الجهاز

أخيرًا ، ابدأ عملية الاقتران:

```
$ idevicepair pair

SUCCESS: Paired with device
c878879d96a910457a3007098693feee2d5XXXXXX
```

الآن ، يمكنك بدء عملية النسخ الاحتياطي .من أجل جمع المزيد من المعلومات المفيدة لتحديد أنشطة Pegasus، أقترح تمكين تشفير النسخ الاحتياطي

(تحتوي النسخة الاحتياطية المشفرة على بيانات أكثر من النسخ الاحتياطية غير المشفرة):

```
$ idevicebackup2 backup encryption on

$ idevicebackup2 backup --full ~/iOSBackup/
```

بمجرد اكتمال عملية النسخ الاحتياطي ، يمكنك بدء التحليل باستخدام أداة mvt-ios
أولاً ، تحتاج إلى *فك تشفير* النسخة الاحتياطية:

```
mvt-ios decrypt-backup -p password -d  ~/iOSBackupDecrypted
~/iOSBackup/
```

تحتاج لبدء استخراج البيانات :

```
mvt-ios check-backup --output ~/MVTOutputs ~/iOSBackupDecrypted/udid/
```

سينشئ هذا الأمر بعض ملفات JSON التي تحتوي على نتائج الاستخراج

تفريغ نظام الملفات

من أجل الحصول على نظام ملفات كامل ، يرجى الرجوع إلى رسالتي السابقة iOS Forensic: الحصول على القرص الكامل باستخدام checkra1n jailbreak.
بمجرد اكتمال عملية الاستحواذ ، يمكنك بدء عملية التحليل باستخدام : *mvt-ios*

II7MAD99@GMAIL.COM 26 Oct 2021


```
mvt-ios check-fs /path/to/filesystem/dump/ --output /path/to/output/
```

السجلات المستخرجة بواسطةmvt-ios

يمكن تحليل جميع البيانات المستخرجة بواسطة mvt-ios

وفقًا لقائمة Pegasus IoC المنشورة بواسطة "Pegasus Project"

البيانات المستخرجة تشمل:

١. : **cache_files.json** سجلات من جميع ملفات قاعدة بيانات SQLite المخزنة على القرص باسم Cache.db. تحتوي قواعد البيانات هذه عادةً على بيانات من التخزين المؤقت لعنوان URL الداخلي لنظام iOS

٢. : **calls.json** سجلات من قاعدة بيانات SQLite الموجودة على *private/var/mobile/Library/CallHistoryDB/CallHistory.storedata* والتي تحتوي على سجلات المكالمات الواردة والصادرة ، بما في ذلك من تطبيقات المراسلة مثل WhatsAppأو.Skype

٣. : **chrome_favicon.json** سجلات من قاعدة بيانات SQLite الموجودة في

*private / var / mobile / Containers / Data / Application / * / Library / Application Support / Google / Chrome / Default / Favicons*

والتي تحتوي على تعيين لعناوين URL المفضلة والأرقام التي تمت زيارتها عناوين المواقع التي تم تحميلها

٤. : **chrome_history.json** سجلات من قاعدة بيانات SQLite الموجودة في

*private / var / mobile / Containers / Data / Application / * / Library / Application Support / Google / Chrome / Default / History*

والتي تحتوي على سجل زيارات.URL

٥. : **contacts.json** سجلات من قاعدة بيانات SQLite الموجودة في *private/var/mobile/Library/AddressBook/AddressBook.sqlitedb* والتي تحتوي على سجلات من دفتر عناوين الهاتف

II7MAD99@GMAIL.COM 26 Oct 2021

٦. : **firefox_favicon.json** سجلات من قاعدة بيانات SQLite الموجودة في *private/var/mobile/profile.profile/browser.db* والتي تحتوي على تعيين لعناوين URL*للأفضلية* وعناوين URL التي تمت زيارتها والتي تم تحميلها

٧. : **firefox_history.json** سجلات من قاعدة بيانات SQLite الموجودة في private/var/mobile/profile.profile/browser.db والتي تحتوي على محفوظات زيارات.URL

٨. : **id_status_cache.json** سجلات من ملف plist الموجود في

private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist

والذي يحتوي على ذاكرة تخزين مؤقت لمصادقة معرف مستخدم .Apple ستشير هذه الفرصة إلى متى قامت تطبيقات مثل Facetime و iMessage بإنشاء جهات اتصال لأول مرة بمعرفات Apple المسجلة الأخرى

٩. : **interaction_c.json** سجلات من قاعدة بيانات SQLite تقع في *private/var/mobile/Library/CoreDuet/People/interactionC.db* والذي يحتوي على تفاصيل حول تفاعلات المستخدم مع التطبيقات المثبتة

١٠. : **locationd_clients.json** سجلات من ملف plist الموجود في *private/var/mobile/Library/Caches/locationd/clients.plist/* والذي يحتوي على ذاكرة تخزين مؤقت للتطبيقات التي طلبت الوصول إلى خدمات الموقع

١١. : **manifest.json** سجلات من قاعدة بيانات SQLite Manifest.db الموجودة في نُسخ iTunes الاحتياطية ، والتي تفهرس الملفات التي تم نسخها احتياطيًا محليًا إلى المسارات الأصلية على جهاز iOS

١٢. : **datausage.json** سجلات من قاعدة بيانات SQLite الموجودة *private/var/wireless/Library/Databases/DataUsage.sqlite* والتي تحتوي على تاريخ استخدام البيانات من خلال العمليات التي تعمل على النظام

١٣. : **netusage.json** سجلات من قاعدة بيانات SQLite الموجودة *private/var/networkd/netusage.sqlite*، والتي تحتوي على تاريخ استخدام البيانات من خلال العمليات التي تعمل على النظام

١٤. : **safari_browser_state.json** سجلات من قواعد بيانات SQLite الموجودة في

private/var/mobile/Library/Safari/BrowserState.db

II7MAD99@GMAIL.COM 26 Oct 2021

أو

private/var/mobile/Containers/Data/Application//Library/Safari/BrowserState.db*

والتي تحتوي على سجلات علامات التبويب المفتوحة

١٥. : **safari_favicon.json** سجلات من قواعد بيانات SQLite الموجودة في

private / var / mobile / Library / Image Cache / Favicons / Favicons.db

أو

*private / var / mobile / Containers / Data / Application / * / Library / Image Cache / Favicons /Favicons.db*

التي تحتوي على تعيينات لعناوين URL*للأفضلات* وعناوين URL التي تمت زيارتها والتي تم تحميلها

١٦. : **safari_history.json** سجلات من قواعد بيانات SQLite الموجودة في

private/var/mobile/Library/Safari/History.db

أو

private/var/mobile/Containers/Data/Application//Library/Safari/History.db*

والتي تحتوي على تاريخ زيارات.URL

١٧. : **sms.json** قائمة رسائل SMS التي تحتوي على روابط HTTP من قاعدة بيانات SQLite الموجودة في

private/var/mobile/Library/SMS/sms.db

١٨. : **sms_attachments.json** تفاصيل حول المرفقات المرسلة عبر SMS أو iMessage من نفس قاعدة البيانات التي تستخدمها وحدة.SMS

١٩. : **version_history.json** سجلات تحديثات برامج iOS من ملفات التحليلات الموجودة في

private/var/db/analyticsd/Analytics-Journal-.ips.*

٢٠. : **webkit_indexeddb.json** قائمة بأسماء الملفات والمجلدات الموجودة في المسار التالي

II7MAD99@GMAIL.COM 26 Oct 2021

*private / var / mobile / Containers / Data / Application / * / Library / WebKit / WebsiteData / IndexedDB*

والتي تحتوي على ملفات IndexedDB التي تم إنشاؤها بواسطة أي تطبيق مثبت على الجهاز

٢١. : **webkit_local_storage.json** قائمة بأسماء الملفات والمجلدات الموجودة في المسار التالي

*private / var / mobile / Containers / Data / Application / * / Library / WebKit / WebsiteData / LocalStorage /*

والتي تحتوي على ملفات تخزين محلية تم إنشاؤها بواسطة أي تطبيق مثبت عليه الجهاز

٢٢. : **webkit_safari_view_service.json** قائمة بأسماء الملفات والمجلدات الموجودة في المسار التالي

private/var/mobile/Containers/Data/Application//SystemData/com.apple.SafariViewService/Library/WebKit/WebsiteData/*

والتي تحتوي على الملفات المخزنة مؤقتًا بواسطة SafariVewService

٢٣. : **webkit_session_resource_log.json** سجلات من ملفات plist بالاسم full_browsing_session_resourceLog.plist، والتي تحتوي على سجلات للموارد التي تم تحميلها بواسطة نطاقات مختلفة تمت زيارتها

٢٤. : **whatsapp.json** قائمة رسائل WhatsApp التي تحتوي على روابط HTTP من قاعدة بيانات SQLite الموجودة في

private/var/mobile/Containers/Shared/AppGroup//ChatStorage.sqlite*

تستطيع فحص المسارات من خلال أداة Fillza بواسطة الايفون

مراجع

١. **تقرير منهجية الطب الشرعي: كيفية التقاط بيغاسوس التابع لمجموعةNSO**
٢. **https://github.com/mvt-project/mvt**
٣. **iOS Forensic: الحصول على القرص الكامل باستخدامcheckra1n jailbreak**
٤. **مؤشر بيغاسوس لمجموعة NSO للتسوية**
٥. **iOS Forensics: كيفية إجراء اكتساب منطقي باستخدامlibimobiledevice**

II7MAD99@GMAIL.COM 26 Oct 2021

استرجاع البيانات بواسطة برنامج PhotoRec

برنامج PhotoRec هو برنامج لاستعادة بيانات الملفات مصمم لاستعادة الملفات المفقودة بما في ذلك الفيديو والمستندات والمحفوظات من الأقراص الثابتة والأقراص المضغوطة والصور المفقودة (وبالتالي اسم استعادة الصور) من ذاكرة الكاميرا الرقمية .يتجاهل برنامج PhotoRec نظام الملفات ويتبع البيانات الأساسية ، لذلك سيستمر العمل حتى إذا كان نظام ملفات الوسائط لديك قد تعرض لأضرار بالغة أو أعيد تنسيقه PhotoRec .هو برنامج مصاحب لـ TestDisk ، وهو تطبيق لاستعادة الأقسام المفقودة على مجموعة متنوعة من أنظمة الملفات وجعل الأقراص غير القابلة للتمهيد قابلة للتمهيد مرة أخرى بالنسبة للأقسام المفقودة / المحذوفة أو الملفات المحذوفة من نظام ملفات FAT أو NTFS ، جرب TestDisk أولاً - عادةً ما يكون أسرع ويمكن لـ TestDisk استرداد أسماء الملفات الأصلية

الاستخدام بسيط حقًا: يمكنك اتباع الدليل المفيد على موقع CGProject أو هذا الفيديو:
https://www.youtube.com/watch?v=EJdx2ORi3r4

لذلك ، فإن أفضل طريقة لتنظيم هذه الملفات هي ترتيبها حسب التاريخ والامتداد .لأداء هذه المهمة الشاقة ، اقتراحي هو استخدام نص بيثون تم تطويره في الأصل بواسطة Chris Magnuson وتحسينه بواسطة

Sort -PhotorecRecoveredFiles [4] . Lukas Hahmann

يقوم هذا البرنامج بنسخ الملفات إلى المجلدات الخاصة بكل نوع ملف .بعد ذلك ، يتم تمييز الملفات حسب السنة ، وفي حال كان الملف المسترد صورة ، حسب الشهر أيضًا عند التقاطها وحسب الحدث .إذا لم يتم اكتشاف تاريخ من الماضي ، يتم وضع ملفات jpg هذه في مجلد واحد ليتم فرزها يدويًا

قم أولاً بتثبيت الحزمة: *exifread*

II7MAD99@GMAIL.COM 26 Oct 2021


```
pip install exifread
```

```
git clone https://github.com/tfrdidi/sort-PhotorecRecoveredFiles
```

إستعمال

```
python recovery.py <path to files recovered by Photorec>
<destination>
```

مراجع

١. Photorec
٢. TestDisk
٣. PhotoRec Step By Step
٤. https://github.com/tfrdidi/sort-PhotorecRecoveredFiles

II7MAD99@GMAIL.COM 26 Oct 2021

جمع معلومات التطبيق

تتمثل إحدى الخطوات الأساسية عند تحليل التطبيقات في جمع المعلومات يمكن القيام بذلك عن طريق فحص حزمة التطبيق على الكمبيوتر المضيف أو عن بُعد من خلال الوصول إلى بيانات التطبيق على الجهاز .ستجد المزيد من التقنيات المتقدمة في الفصول اللاحقة ، ولكن في الوقت الحالي ، سنركز على الأساسيات: الحصول على قائمة بجميع التطبيقات المثبتة ، واستكشاف حزمة التطبيق والوصول إلى أدلة بيانات التطبيق على الجهاز نفسه .يجب أن يمنحك هذا القليل من السياق حول ما يدور حوله التطبيق دون الحاجة إلى إجراء هندسة عكسية له أو إجراء تحليل أكثر تقدمًا سوف نجيب على أسئلة مثل:

- **ما هي الملفات المضمنة في الحزمة؟**
- **ما هي الأطر التي يستخدمها التطبيق؟**
- **ما هي الإمكانيات التي يتطلبها التطبيق؟**
- **ما هي الأذونات التي يطلبها التطبيق من المستخدم ولأي سبب؟**
- **هل يسمح التطبيق بأي اتصالات غير آمنة؟**
- **هل يقوم التطبيق بإنشاء أي ملفات جديدة عند تثبيته؟**

شرحت سابقا كيف نستخرج الدايلب من اداة Frida :

```
$ frida-ps -Uai

PID  Name                 Identifier
----  -------------------  ----------------------------------------
6847  Calendar             com.apple.mobilecal
6815  Mail                 com.apple.mobilemail
   -  App Store            com.apple.AppStore
   -  Apple Store          com.apple.store.Jolly
   -  Calculator           com.apple.calculator
   -  Camera               com.apple.camera
   -  iGoat-Swift          OWASP.iGoat-Swift
```

II7MAD99@GMAIL.COM 26 Oct 2021

الان نريد استكشاف حزمة التطبيق نكتب الدايلب المراد استكشاف ملفاته

في أداة frida-ios-dump سبق وشرحتها (نحمل التطبيق بصيغة IPA)

ويمكنك فك ضغط IPA باستخدام المعيار unzip أو أي أداة ZIP أخرى ستجد Payload بالداخل مجلدًا يحتوي على ما يسمى بـ Application Bundle (.app).فيما يلي مثال في الإخراج التالي ، لاحظ أنه تم اقتطاعه لتحسين إمكانية القراءة والنظرة العامة:

```
$ ls -1 Payload/iGoat-Swift.app
```

العناصر الأكثر صلة هي:

- **Info.plist يحتوي على معلومات التكوين الخاصة بالتطبيق ، مثل معرف الحزمة الخاص به ورقم الإصدار واسم العرض.**
- **_CodeSignature/ يحتوي على ملف plist بتوقيع على جميع الملفات في الحزمة**
- **Frameworks/ يحتوي على مكتبات التطبيق الأصلية كملفات dylib. أو framework.**
- **PlugIns/ قد تحتوي على إضافات التطبيقات كملفات appex غير موجودة في المثال**
- **iGoat-Swift هو البرنامج الثنائي الذي يحتوي على رمز التطبيق .اسمها هو نفس اسم الحزمة مطروحًا منه ملحق.app.**
- **موارد مختلفة مثل الصور / الرموز *.nib والملفات) تخزين واجهات المستخدم لتطبيق (iOS والمحتوى المترجم (<language>.lproj) والملفات النصية والملفات الصوتية وما إلى ذلك**

ملف Info.plist

قائمة خصائص المعلومات أو Info.plist (المسماة حسب الاصطلاح) هي المصدر الرئيسي للمعلومات لتطبيق .iOS يتكون من ملف منظم يحتوي على أزواج مفتاح -

II7MAD99@GMAIL.COM 26 Oct 2021

قيمة تصف معلومات التكوين الأساسية حول التطبيق .في الواقع ، من المتوقع أن تحتوي جميع الملفات التنفيذية المجمعة (امتدادات التطبيقات وأطر العمل والتطبيقات) على Info.plist ملف يمكنك العثور على جميع المفاتيح الممكنة في وثائق مطور Apple .
يمكن تنسيق الملف بتنسيق XML أو ثنائي .(bplist) يمكنك تحويله إلى تنسيق XML بأمر واحد بسيط:

على نظام macOS plutil ، وهي أداة تأتي أصلاً مع macOS 10.2 والإصدارات الأحدث

(لا تتوفر حاليًا وثائق رسمية عبر الإنترنت):

```
plutil $ -convert xml1 Info.plist
```

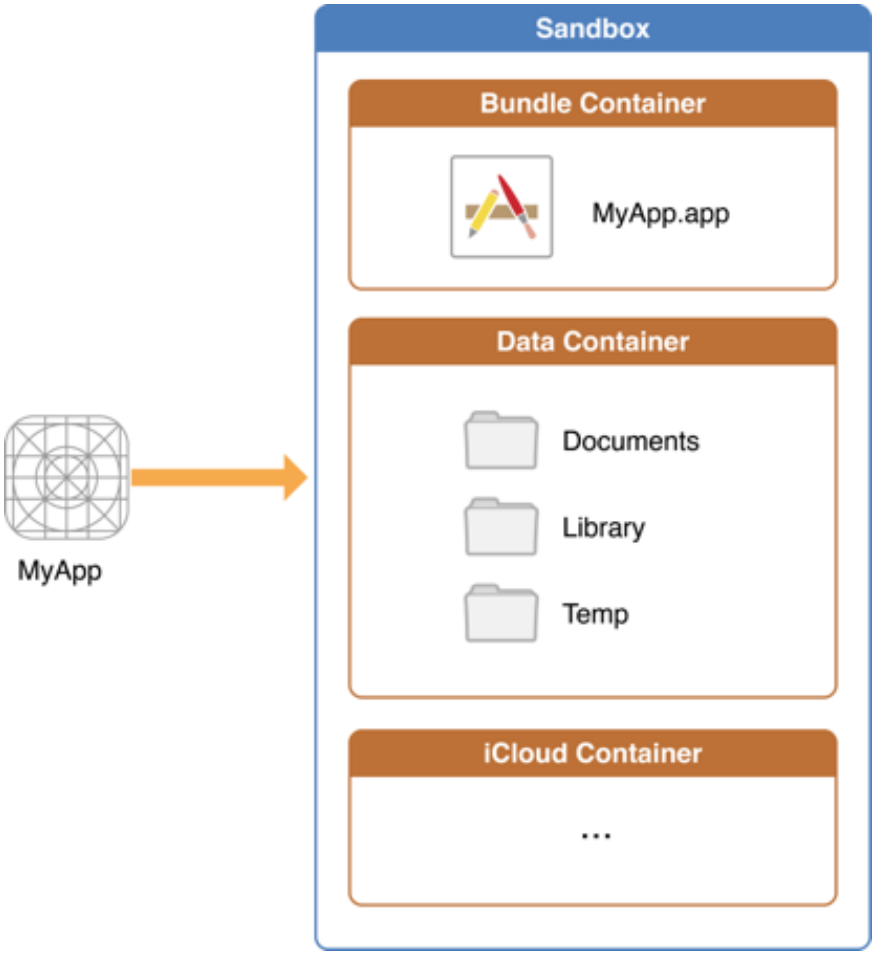
على نظام: Linux

```
$ apt install libplist-utils
$ plistutil -i Info.plist -o Info_xml.plist
```

فيما يلي قائمة غير شاملة لبعض المعلومات والكلمات الرئيسية المقابلة التي يمكنك البحث عنها بسهولة في Info.plist بمجرد فحص الملف

II7MAD99@GMAIL.COM 26 Oct 2021

بمجرد تثبيت التطبيق ، هناك المزيد من المعلومات لاستكشافها دعنا نلقي نظرة عامة موجزة على بنية مجلد التطبيق في تطبيقات iOS لفهم البيانات التي يتم تخزينها في المكان .يمثل الرسم التوضيحي التالي بنية مجلد التطبيق:



على نظام iOS ، يمكن العثور على تطبيقات النظام في Applications الدليل بينما تتوفر التطبيقات المثبتة من قبل المستخدم ضمن private/var/containers/ ومع ذلك ، فإن العثور على المجلد الصحيح فقط من خلال التنقل في نظام الملفات ليس مهمة تافهة حيث يحصل كل تطبيق على UUID عشوائي ١٢٨ بت (المعرف الفريد العالمي) مخصص لأسماء الدلائل الخاصة به.
من أجل الحصول بسهولة على معلومات دليل التثبيت للتطبيقات التي يثبتها المستخدم ، يمكنك اتباع الطرق التالية:

قم بالاتصال بالجهاز الترمينال على الجهاز الايفون وقم بتشغيل الأمر ipainstaller
https://cydia.saurik.com/package/com.autopear.installipa

II7MAD99@GMAIL.COM 26 Oct 2021

(IPA Installer Console) كما يلي:

```
iPhone:~ root# ipainstaller -l
...
OWASP.iGoat-Swift

iPhone:~ root# ipainstaller -i OWASP.iGoat-Swift
...
Bundle: /private/var/containers/Bundle/Application/3ADAF47D-A734-
49FA-B274-FBCA66589E67
Application: /private/var/containers/Bundle/Application/3ADAF47D-
A734-49FA-B274-FBCA66589E67/iGoat-Swift.app
Data: /private/var/mobile/Containers/Data/Application/8C8E7EB0-BC9B-
435B-8EF8-8F5560EB0693
```

سيؤدي استخدام أمر الاعتراض أيضًا إلى إظهار جميع معلومات الدليل الخاصة بالتطبيق .الاتصال بالتطبيق مع الاعتراض

```
OWASP.iGoat-Swift on (iPhone: 11.1.2) [usb] # env

Name                Path
-----------------  -------------------------------------------------------
-------------------------------------
BundlePath          /var/containers/Bundle/Application/3ADAF47D-A734-49FA-
B274-FBCA66589E67/iGoat-Swift.app
CachesDirectory     /var/mobile/Containers/Data/Application/8C8E7EB0-BC9B-
435B-8EF8-8F5560EB0693/Library/Caches
DocumentDirectory   /var/mobile/Containers/Data/Application/8C8E7EB0-BC9B-
435B-8EF8-8F5560EB0693/Documents
LibraryDirectory    /var/mobile/Containers/Data/Application/8C8E7EB0-BC9B-
435B-8EF8-8F5560EB0693/Library
```

كما ترى ، فإن التطبيقات لها موقعان رئيسيان:

- دليل الحزمة (/var/containers/Bundle/Application/3ADAF47D-A734-49FA-B274-FBCA66589E67/).

II7MAD99@GMAIL.COM 26 Oct 2021

- دليل البيانات
(/var/mobile/Containers/Data/Application/8C8E7EB0-BC9B-435B-8EF8-8F5560EB0693/).

تحتوي هذه المجلدات على معلومات يجب فحصها عن كثب أثناء تقييمات أمان التطبيق (على سبيل المثال عند تحليل البيانات المخزنة لبيانات حساسة).

دليل الحزمة:

- AppName.app
  - هذه هي حزمة التطبيقات كما رأينا من قبل في IPA ، فهي تحتوي على بيانات التطبيق الأساسية والمحتوى الثابت بالإضافة إلى البرنامج الثنائي المترجم للتطبيق.
  - هذا الدليل مرئي للمستخدمين ، لكن لا يمكنهم الكتابة إليه.
  - لم يتم نسخ المحتوى في هذا الدليل احتياطيًا.
  - يتم استخدام محتويات هذا المجلد للتحقق من صحة توقيع الرمز.

دليل البيانات:

- وثائق/
  - يحتوي على جميع البيانات التي تم إنشاؤها بواسطة المستخدم .يبدأ المستخدم النهائي للتطبيق في إنشاء هذه البيانات.
  - مرئي للمستخدمين ويمكن للمستخدمين الكتابة إليه.
  - المحتوى في هذا الدليل تم نسخه احتياطيًا.
  - يمكن للتطبيق تعطيل المسارات عن طريق الضبط .NSURLIsExcludedFromBackupKey
- مكتبة/
  - يحتوي على جميع الملفات غير الخاصة بالمستخدم ، مثل ذاكرات التخزين المؤقت والتفضيلات وملفات تعريف الارتباط وملفات تكوين قائمة الخصائص.(plist)
  - تستخدم تطبيقات iOS عادةً الدلائل الفرعية Application Support وCaches، ولكن يمكن للتطبيق إنشاء أدلة فرعية مخصصة.
- مكتبة / مخابئ/
  - يحتوي على ملفات مخزنة مؤقتًا شبه دائمة.
  - غير مرئي للمستخدمين ولا يمكن للمستخدمين الكتابة إليه.
  - لم يتم نسخ المحتوى في هذا الدليل احتياطيًا.

II7MAD99@GMAIL.COM 26 Oct 2021

- قد يحذف نظام التشغيل ملفات هذا الدليل تلقائيًا عندما لا يكون التطبيق قيد التشغيل وتقل مساحة التخزين.

- المكتبة / دعم التطبيق/
  - يحتوي على ملفات ثابتة ضرورية لتشغيل التطبيق.
  - غير مرئي للمستخدمين ولا يمكن للمستخدمين الكتابة إليه.
  - المحتوى في هذا الدليل تم نسخه احتياطيًا.
  - يمكن للتطبيق تعطيل المسارات عن طريق الضبط NSURLIsExcludedFromBackupKey.
- المكتبة / التفضيلات/
  - يستخدم لتخزين الخصائص التي يمكن أن تستمر حتى بعد إعادة تشغيل التطبيق.
  - يتم حفظ المعلومات ، غير مشفرة ، داخل آلية تحديد الحماية للتطبيق في ملف plist يسمى.plist. [BUNDLE_ID]
  - NSUserDefaultsيمكن العثور على جميع أزواج المفاتيح / القيمة المخزنة باستخدام في هذا الملف.
- tmp /
  - استخدم هذا الدليل لكتابة ملفات مؤقتة لا تحتاج إلى الاستمرار بين عمليات تشغيل التطبيق.
  - يحتوي على ملفات مخزنة مؤقتًا غير دائمة.
  - غير مرئي للمستخدمين.
  - لم يتم نسخ المحتوى في هذا الدليل احتياطيًا.
  - قد يحذف نظام التشغيل ملفات هذا الدليل تلقائيًا عندما لا يكون التطبيق قيد التشغيل وتقل مساحة التخزين.

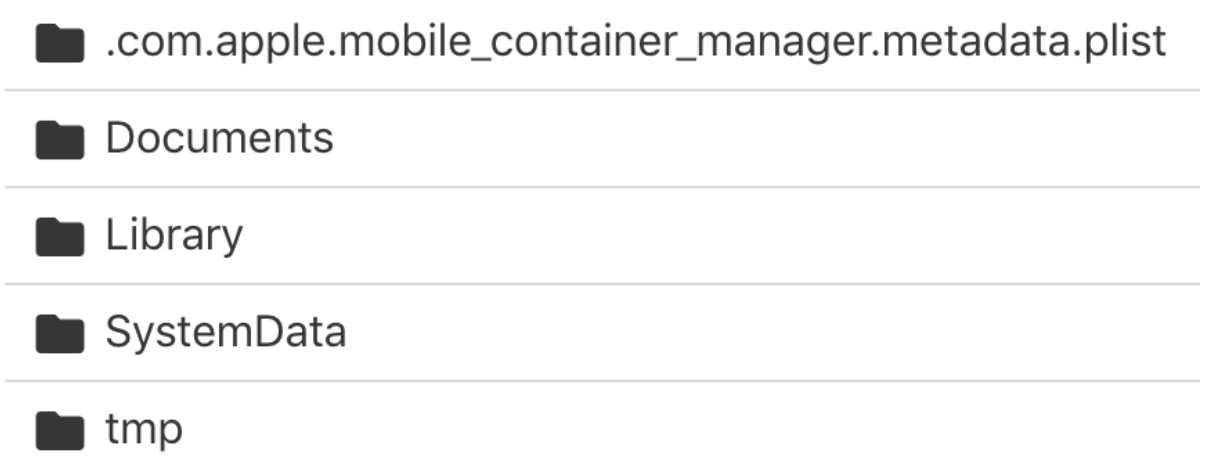
دعنا نلقي نظرة فاحصة على دليل حزمة تطبيقات (iGoat-Swift (.app داخل دليل الحزمة

(/var/containers/Bundle/Application/3ADAF47D-A734-49FA-B274-FBCA66589E67/iGoat-Swift.app)

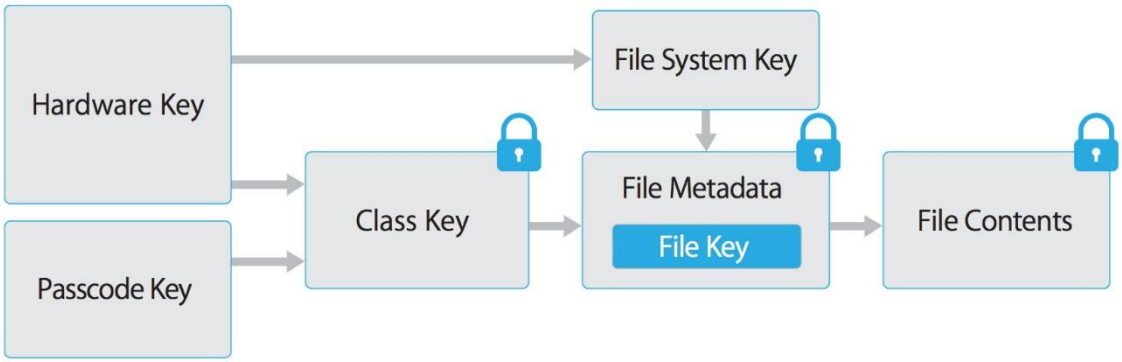
```
OWASP.iGoat-Swift on (iPhone: 11.1.2) [usb] # ls
NSFileType      Perms  NSFileProtection    ...  Name
------------  -------  ------------------  ...  ----------------------------------
----
Regular           420  None                ...  rutger.html
Regular           420  None                ...  mansi.html
Regular           420  None                ...  splash.html
Regular           420  None                ...  about.html
```

II7MAD99@GMAIL.COM 26 Oct 2021


```
Regular          420  None                ...  LICENSE.txt
Regular          420  None                ...  Sentinel.txt
Regular          420  None                ...  README.txt

Directory        493  None                ...  URLSchemeAttackExerciseVC.nib
Directory        493  None                ...  CutAndPasteExerciseVC.nib
Directory        493  None                ...  RandomKeyGenerationExerciseVC.nib
Directory        493  None                ...  KeychainExerciseVC.nib
Directory        493  None                ...  CoreData.momd
Regular          420  None                ...  archived-expanded-
entitlements.xcent
Directory        493  None                ...  SVProgressHUD.bundle

Directory        493  None                ...  Base.lproj
Regular          420  None                ...  Assets.car
Regular          420  None                ...  PkgInfo
Directory        493  None                ...  _CodeSignature
Regular          420  None                ...  AppIcon60x60@3x.png

Directory        493  None                ...  Frameworks

Regular          420  None                ...  embedded.mobileprovision

Regular          420  None                ...  Credentials.plist
Regular          420  None                ...  Assets.plist
Regular          420  None                ...  Info.plist

Regular          493  None                ...  iGoat-Swift
```



II7MAD99@GMAIL.COM 26 Oct 2021



تخزين بيانات iOS

تعد حماية البيانات الحساسة ، مثل رموز المصادقة والمعلومات الخاصة ، أمرًا أساسيًا لأمان الهاتف المحمول .في هذا الفصل ، ستتعرف على واجهات برمجة تطبيقات iOS لتخزين البيانات المحلية وأفضل الممارسات لاستخدامها

واجهة برمجة تطبيقات حماية البيانات

يمكن لمطوري التطبيقات الاستفادة من واجهات برمجة تطبيقات *حماية بيانات* iOSلتنفيذ تحكم دقيق في الوصول لبيانات المستخدم المخزنة في ذاكرة فلاش .تم تصميم واجهات برمجة التطبيقات أعلى معالج المنطقة الآمنة Secure Enclave Processor (SEP)، والذي تم تقديمه مع iPhone 5S. SEP هو معالج مساعد يوفر عمليات تشفير لحماية البيانات وإدارة المفاتيح .يتم تضمين مفتاح الأجهزة الخاص بالجهاز - المعرف الفريد للجهاز - في الجيب الآمن ، مما يضمن سلامة حماية البيانات حتى في حالة تعرض نواة نظام التشغيل للخطر.

تستند بنية حماية البيانات إلى تسلسل هرمي للمفاتيح .يقع UID ومفتاح رمز مرور المستخدم) المشتق من عبارة مرور المستخدم عبر خوارزمية (PBKDF2 في أعلى هذا التسلسل الهرمي .يمكن استخدامهما معًا "لإلغاء تأمين" ما يسمى بمفاتيح الفئة ، والتي ترتبط بحالة الجهاز المختلفة (على سبيل المثال ، الجهاز مغلق / غير مقفل).

يتم تشفير كل ملف مخزن على نظام ملفات iOS باستخدام مفتاح كل ملف خاص به ، والذي يتم تضمينه في البيانات الوصفية للملف .يتم تشفير البيانات الوصفية باستخدام

II7MAD99@GMAIL.COM 26 Oct 2021

مفتاح نظام الملفات وتغليفها بمفتاح الفئة المطابق لفئة الحماية التي حددها التطبيق عند إنشاء الملف

https://support.apple.com/en-sa/guide/security/welcome/web

الحماية الكاملة : (NSFileProtectionComplete) مفتاح مشتق من رمز مرور المستخدم والمعرف الفريد للجهاز يحمي مفتاح الفئة هذا .يتم مسح المفتاح المشتق من الذاكرة بعد فترة وجيزة من قفل الجهاز ، مما يجعل الوصول إلى البيانات غير ممكن حتى يفتح المستخدم قفل الجهاز.

محمية ما لم يتم فتحها

: (NSFileProtectionCompleteUnlessOpen) فئة الحماية هذه مشابهة للحماية الكاملة ، ولكن إذا تم فتح الملف عند إلغاء القفل ، يمكن للتطبيق الاستمرار في الوصول إلى الملف حتى إذا قام المستخدم بإغلاق الجهاز .يتم استخدام فئة الحماية هذه ، على سبيل المثال ، عند تنزيل مرفق بريد في الخلفية.

محمية حتى مصادقة المستخدم الأول

: (NSFileProtectionCompleteUntilFirstUserAuthentication) يمكن الوصول إلى الملف بمجرد أن يفتح المستخدم الجهاز لأول مرة بعد التمهيد .يمكن الوصول إليه حتى إذا قام المستخدم بعد ذلك بإغلاق الجهاز ولم تتم إزالة مفتاح الفئة من الذاكرة.

بلا حماية : (NSFileProtectionNone) المفتاح الخاص بفئة الحماية هذه محمي بواسطة UID فقط .يتم تخزين مفتاح الفئة في "Effaceable Storage" ، وهي منطقة من ذاكرة الفلاش على جهاز iOS تسمح بتخزين كميات صغيرة من البيانات .توجد فئة الحماية هذه للمسح السريع عن بُعد (الحذف الفوري لمفتاح الفئة ، مما يجعل الوصول إلى البيانات غير ممكن).

II7MAD99@GMAIL.COM 26 Oct 2021

NSFileProtectionNone يتم تشفير جميع مفاتيح الفئات باستثناء مفتاح مشتق من UID الخاص بالجهاز ورمز مرور المستخدم .نتيجة لذلك ، يمكن أن يحدث فك التشفير فقط على الجهاز نفسه ويتطلب رمز المرور الصحيح.

منذ iOS 7 ، فئة حماية البيانات الافتراضية هي "محمية حتى مصادقة المستخدم الأول."

سلسلة المفاتيح

يمكن استخدام سلسلة مفاتيح iOS لتخزين أجزاء صغيرة وحساسة من البيانات بأمان ، مثل مفاتيح التشفير ورموز الجلسة .يتم تنفيذه كقاعدة بيانات SQLite التي يمكن الوصول إليها من خلال واجهات برمجة تطبيقات Keychain فقط.

في نظام macOS ، يمكن لكل تطبيق مستخدم إنشاء العديد من سلاسل المفاتيح حسب الرغبة ، ولكل حساب تسجيل دخول سلسلة مفاتيح خاصة به .يختلف هيكل Keychain على iOS : يتوفر Keychain واحد فقط لجميع التطبيقات .يمكن مشاركة الوصول إلى العناصر بين التطبيقات الموقعة من قبل نفس المطور عبر ميزة مجموعات الوصول الخاصة بالسمة kSecAttrAccessGroup. وتمكن من الوصول إلى المفاتيح التي securityd الخفي، الذي يمنح الوصول وفقا لالتطبيق Keychain-access-groups، application-identifier وapplication-group الاستحقاقات.

تتضمن Keychain API العمليات الرئيسية التالية:

SecItemAdd

SecItemUpdate

SecItemCopyMatching

SecItemDelete

تتم حماية البيانات المخزنة في Keychain عبر بنية فئة مشابهة لهيكل الفئة المستخدم لتشفير الملفات .العناصر المضافة إلى Keychain يتم ترميزها على أنها plist ثنائية ويتم تشفيرها باستخدام مفتاح AES 128 بت لكل عنصر في Galois / Counter Mode (GCM). لاحظ أن الكتل الكبيرة من البيانات لا يُقصد حفظها مباشرة في Keychain - وهذا هو الغرض من Data Protection API. يمكنك تكوين حماية البيانات لعناصر Keychain عن طريق تعيين kSecAttrAccessible المفتاح في المكالمة إلى SecItemAdd أو SecItemUpdate. قيم إمكانية

II7MAD99@GMAIL.COM 26 Oct 2021

الوصول التالية القابلة للتكوين لـ kSecAttrAccessible هي فئات حماية بيانات Keychain:

`kSecAttrAccessibleAlways`: يمكن دائمًا الوصول إلى البيانات الموجودة في عنصر Keychain ، بغض النظر عما إذا كان الجهاز مغلقًا أم لا.

`kSecAttrAccessibleAlwaysThisDeviceOnly`: يمكن دائمًا الوصول إلى البيانات الموجودة في عنصر Keychain ، بغض النظر عما إذا كان الجهاز مغلقًا أم لا .لن يتم تضمين البيانات في iCloud أو نسخة احتياطية محلية.

`kSecAttrAccessibleAfterFirstUnlock`: لا يمكن الوصول إلى البيانات الموجودة في عنصر Keychain بعد إعادة التشغيل حتى يتم إلغاء قفل الجهاز مرة واحدة بواسطة المستخدم.

`kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly`: لا يمكن الوصول إلى البيانات الموجودة في عنصر Keychain بعد إعادة التشغيل حتى يتم إلغاء قفل الجهاز مرة واحدة بواسطة المستخدم .لا يتم ترحيل العناصر التي تحمل هذه السمة إلى جهاز جديد .وبالتالي ، بعد الاستعادة من نسخة احتياطية لجهاز مختلف ، لن تكون هذه العناصر موجودة.

`kSecAttrAccessibleWhenUnlocked`: لا يمكن الوصول إلى البيانات الموجودة في عنصر Keychain إلا أثناء إلغاء قفل الجهاز من قبل المستخدم.

`kSecAttrAccessibleWhenUnlockedThisDeviceOnly`: لا يمكن الوصول إلى البيانات الموجودة في عنصر Keychain إلا أثناء إلغاء قفل الجهاز من قبل المستخدم .لن يتم تضمين البيانات في iCloud أو نسخة احتياطية محلية.

`kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly`: لا يمكن الوصول إلى البيانات الموجودة في Keychain إلا عند إلغاء قفل الجهاز .لا تتوفر فئة الحماية هذه إلا إذا تم تعيين رمز مرور على الجهاز .لن يتم تضمين البيانات في iCloudأو نسخة احتياطية محلية.

`AccessControlFlags` تحديد الآليات التي يمكن للمستخدمين من خلالها مصادقة المفتاح:(`SecAccessControlCreateFlags`)

`kSecAccessControlDevicePasscode`: الوصول إلى العنصر عبر رمز مرور.

II7MAD99@GMAIL.COM 26 Oct 2021

kSecAccessControlBiometryAny: الوصول إلى العنصر عبر إحدى بصمات الأصابع المسجلة في Touch ID. لا تؤدي إضافة بصمة إصبع أو إزالتها إلى إلغاء صلاحية العنصر.

kSecAccessControlBiometryCurrentSet: الوصول إلى العنصر عبر إحدى بصمات الأصابع المسجلة في Touch ID إضافة بصمة إصبع أو إزالتها إلى إبطال العنصر.

kSecAccessControlUserPresence: الوصول إلى العنصر عبر إحدى بصمات الأصابع المسجلة) باستخدام (Touch ID أو افتراضيًا على رمز المرور

يرجى ملاحظة أن المفاتيح المؤمنة بواسطة Touch ID

عبر kSecAccessControlBiometryAnyأو kSecAccessControlB iometryCurrentSet)محمية بواسطة: Secure Enclave تحمل Keychain رمزًا مميزًا فقط ، وليس المفتاح الفعلي .يكمن المفتاح في المنطقة الآمنة Secure Enclave.

بدءًا من iOS 9 ، يمكنك القيام بعمليات التوقيع المستندة إلى ECC في Secure Enclave.في هذا السيناريو ، يوجد المفتاح الخاص وعمليات التشفير داخل Secure Enclave.راجع قسم التحليل الثابت لمزيد من المعلومات حول إنشاء مفاتيح ECC.يدعم iOS 9 فقط ٢٥٦ بت .ECC علاوة على ذلك ، تحتاج إلى تخزين المفتاح العام في Keychain لأنه لا يمكن تخزينه في .Secure Enclave بعد إنشاء المفتاح ، يمكنك استخدام kSecAttrKeyType للإشارة إلى نوع الخوارزمية التي تريد استخدام المفتاح معها

في حالة رغبتك في استخدام هذه الآليات ، يوصى باختبار ما إذا كان قد تم تعيين رمز المرور أم لا .في نظام التشغيلiOS 8 ، ستحتاج إلى التحقق مما إذا كان بإمكانك القراءة / الكتابة من عنصر في Keychain المحمي بواسطة

kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

السمة .بدءًا من نظام التشغيل iOS 9 وما بعده ، يمكنك التحقق مما إذا كانت شاشة القفل مضبوطة أم لا ، باستخدام : LAContext

II7MAD99@GMAIL.COM 26 Oct 2021

Swift:

```
public func devicePasscodeEnabled() -> Bool {
    return LAContext().canEvaluatePolicy(.deviceOwnerAuthentication,
error: nil)
}
```

Objective-C:

```
-(BOOL)devicePasscodeEnabled:(LAContex)context{
  if ([context canEvaluatePolicy:LAPolicyDeviceOwnerAuthentication
error:nil]) {
        return true;
    } else {
        return false;
    }
}
```

ثبات بيانات Keychain

في نظام التشغيل iOS ، عند إلغاء تثبيت أحد التطبيقات ، يحتفظ الجهاز ببيانات Keychain التي يستخدمها التطبيق ، على عكس البيانات المخزنة بواسطة وضع الحماية للتطبيق الذي يتم مسحه .في حالة قيام المستخدم ببيع أجهزته دون إجراء إعادة ضبط المصنع ، فقد يتمكن مشتري الجهاز من الوصول إلى حسابات وبيانات تطبيقات المستخدم السابق عن طريق إعادة تثبيت نفس التطبيقات التي استخدمها المستخدم السابق .هذا لن يتطلب أي قدرة فنية على الأداء.

عند تقييم تطبيق iOS ، يجب أن تبحث عن استمرارية بيانات .Keychain يتم ذلك عادةً باستخدام التطبيق لإنشاء بيانات نموذجية قد يتم تخزينها في Keychain ، وإلغاء تثبيت التطبيق ، ثم إعادة تثبيت التطبيق لمعرفة ما إذا كان قد تم الاحتفاظ بالبيانات بين عمليات تثبيت التطبيق .استخدم مجموعة أدوات استكشاف الهاتف المحمول

II7MAD99@GMAIL.COM 26 Oct 2021

لوقت تشغيل الاعتراض لتفريغ بيانات سلسلة المفاتيح .يوضح objection الأمر التالي هذا الإجراء:

```
... ...itudehacks.DVIAswiftv2.develop on (iPhone: 13.2.3) [usb] # ios keychain dump
Note: You may be asked to authenticate using the devices passcode or TouchID
Save the output by adding `--json keychain.json` to this command
Dumping the iOS keychain...
Created                Accessible                ACL  Type     Account                Service                Data
---------------------- ------------------------- ---- -------- ---------------------- ---------------------- ----------
2020-02-11 13:26:52 +0000  WhenUnlocked                None  Password  keychainValue  com.highaltitudehacks.DVIAswiftv2.develop  mysecretpass123
```

لا توجد واجهة برمجة تطبيقات iOS يمكن للمطورين استخدامها لفرض مسح البيانات عند إلغاء تثبيت أحد التطبيقات .بدلاً من ذلك ، يجب على المطورين اتخاذ الخطوات التالية لمنع استمرار بيانات Keychain بين عمليات تثبيت التطبيق:

- عند تشغيل التطبيق لأول مرة بعد التثبيت ، امسح جميع بيانات Keychain المرتبطة بالتطبيق .سيمنع هذا المستخدم الثاني للجهاز من الوصول بطريق الخطأ إلى حسابات المستخدم السابقة .مثال Swift التالي هو توضيح أساسي لإجراء المسح هذا:

```
let userDefaults = UserDefaults.standard

if userDefaults.bool(forKey: "hasRunBefore") == false {
    // Remove Keychain items here

    // Update the flag indicator
    userDefaults.set(true, forKey: "hasRunBefore")
    userDefaults.synchronize() // Forces the app to update UserDefaults
}
```

- عند تطوير وظيفة تسجيل الخروج لتطبيق iOS ، تأكد من مسح بيانات Keychain كجزء من تسجيل الخروج من الحساب .سيسمح هذا للمستخدمين بمسح حساباتهم قبل إلغاء تثبيت التطبيق

II7MAD99@GMAIL.COM 26 Oct 2021

التحليل الديناميكي مع Xcode و iOS simulator

هذا الاختبار متاح فقط على macOS ، حيث يلزم وجود Xcode ومحاكي iOS

لاختبار التخزين المحلي والتحقق من البيانات المخزنة فيه ، ليس من الضروري أن يكون لديك جهاز iOS. من خلال الوصول إلى الكود المصدري و Xcode ، يمكن إنشاء التطبيق ونشره في محاكي iOS. يتوفر نظام الملفات الخاص بالجهاز الحالي لمحاكي iOS بتنسيق
~/Library/Developer/CoreSimulator/Devices
بمجرد تشغيل التطبيق في محاكي iOS ، يمكنك الانتقال إلى دليل أحدث جهاز محاكاة بدأ بالأمر التالي:

```
$ cd ~/Library/Developer/CoreSimulator/Devices/$(
ls -alht ~/Library/Developer/CoreSimulator/Devices | head -n 2 |
awk '{print $9}' | sed -n '1!p')/data/Containers/Data/Application
```

الآن ما زلت بحاجة إلى البحث عن .لأحدث جهاز محاكاة تم تشغيله UUID سيجد الأمر أعلاه تلقائيًا الخاص بالتطبيق UUID سيُظهر لك هذا اسم التطبيق الخاص بك أو كلمة رئيسية في تطبيقك.

```
$ grep -iRn keyword
```

عد ذلك ، يمكنك مراقبة التغييرات في نظام ملفات التطبيق والتحقق منها والتحقق مما إذا كانت أي معلومات حساسة مخزنة داخل الملفات أثناء استخدام التطبيق

II7MAD99@GMAIL.COM 26 Oct 2021

البحث عن ملفات تعريف الارتباط Cookies

بتخزين ملفات تعريف الارتباط الثنائية في وضع الحماية iOS غالبًا ما تقوم تطبيقات ملفات تعريف الارتباط هي ملفات ثنائية تحتوي على بيانات ملفات تعريف .للتطبيق يمكنك استخدام الاعتراض لتحويل هذه الملفات .الارتباط الخاصة بعروض ويب التطبيق وفحص البيانات JSON إلى تنسيق.

```
...itudehacks.DVIAswiftv2.develop on (iPhone: 13.2.3) [usb] # ios cookies get --json
[
    {
        "domain": "highaltitudehacks.com",
        "expiresDate": "2051-09-15 07:46:43 +0000",
        "isHTTPOnly": "false",
        "isSecure": "false",
        "name": "username",
        "path": "/",
        "value": "admin123",
        "version": "0"
    }
]
```

تستخدم تطبيقات iOS عادةً قواعد بيانات SQLite لتخزين البيانات التي يتطلبها التطبيق .يجب على المختبرين التحقق من قيم حماية البيانات لهذه الملفات ومحتوياتها بحثًا عن بيانات حساسة .يحتوي الاعتراض على وحدة للتفاعل مع قواعد بيانات .SQLite يسمح بتفريغ المخطط وجداولهم والاستعلام عن السجلات

```
...itudehacks.DVIAswiftv2.develop on (iPhone: 13.2.3) [usb] # sqlite connect Model.sqlite
Caching local copy of database file...
Downloading /var/mobile/Containers/Data/Application/264C23B8-07B5-4B5D-8701-C020C301C151/Library/Application Support/Model.sqlite to /var/folders/4m/dsg0mq_17g39g473z0996r7m0000gq/T/tmpdr_7rvxi.sqlite
Streaming file from device...
Writing bytes to destination...
Successfully downloaded /var/mobile/Containers/Data/Application/264C23B8-07B5-4B5D-8701-C020C301C151/Library/Application Support/Model.sqlite to /var/folders/4m/dsg0mq_17g39g473z0996r7m0000gq/T/tmpdr_7rvxi.sqlite
Validating SQLite database format
```

II7MAD99@GMAIL.COM 26 Oct 2021


```
Connected to SQLite database at: Model.sqlite

SQLite @ Model.sqlite > .tables
+--------------+
| name         |
+--------------+
| ZUSER        |
| Z_METADATA   |
| Z_MODELCACHE |
| Z_PRIMARYKEY |
+--------------+
Time: 0.013s

SQLite @ Model.sqlite > select * from Z_PRIMARYKEY
+-------+--------+---------+-------+
| Z_ENT | Z_NAME | Z_SUPER | Z_MAX |
+-------+--------+---------+-------+
| 1     | User   | 0       | 0     |
+-------+--------+---------+-------+
1 row in set
Time: 0.013s
```

البحث عن قواعد بيانات ذاكرة التخزين المؤقت

بشكل افتراضي ، يقوم NSURLSession بتخزين البيانات ، مثل طلبات واستجابات HTTP في قاعدة بيانات Cache.db يمكن أن تحتوي قاعدة البيانات هذه على بيانات حساسة ، إذا تم تخزين الرموز المميزة أو أسماء المستخدمين أو أي معلومات حساسة أخرى مؤقتًا .للعثور على المعلومات المخزنة مؤقتًا ، افتح دليل بيانات التطبيق
(/var/mobile/Containers/Data/Application/<UUID>)وانتقل
إلى .<Bundle Identifier>/Library/Caches/يتم أيضًا تخزين ذاكرة التخزين المؤقت WebKitفي ملف Cache.db. يمكن فتح الاعتراض والتفاعل مع قاعدة البيانات باستخدام الأمر SQLite connect Cache.db، حيث إنها قاعدة بيانات SQLite عادية

التوصيات

يوصى بتعطيل التخزين المؤقت لهذه البيانات ، حيث قد تحتوي على معلومات حساسة في الطلب أو الاستجابة توضح القائمة التالية أدناه طرقًا مختلفة لتحقيق ذلك:

يوصى بإزالة الاستجابات المخبأة بعد تسجيل الخروج .يمكن القيام بذلك بالطريقة التي توفرها Apple والتي تسمى removeAllCachedResponses يمكنك استدعاء هذه الطريقة على النحو التالي:

URLCache.shared.removeAllCachedResponses()

ستؤدي هذه الطريقة إلى إزالة كافة الطلبات والاستجابات المخزنة مؤقتًا من ملف.Cache.db

II7MAD99@GMAIL.COM 26 Oct 2021

إذا لم تكن بحاجة إلى استخدام ميزة ملفات تعريف الارتباط ، فمن المستحسن استخدام خاصية التكوين ephemeral.الخاصة بـ URLSession ، والتي ستؤدي إلى تعطيل حفظ ملفات تعريف الارتباط وذاكرة التخزين المؤقت.

وثائق: Apple

An ephemeral session configuration object is similar to a default session configuration (see default), except that the corresponding session object doesn't store caches, credential stores, or any session-related data to disk. Instead, session-related data is stored in RAM. The only time an ephemeral session writes data to disk is when you tell it to write the contents of a URL to a file.

يمكن أيضًا تعطيل ذاكرة التخزين المؤقت عن طريق تعيين نهج ذاكرة التخزين المؤقت على notAllowed. سيعطل تخزين ذاكرة التخزين المؤقت بأي شكل من الأشكال ، سواء في الذاكرة أو على القرص

II7MAD99@GMAIL.COM 26 Oct 2021

مراجعة التعليمات البرمجية اليدوية (Reversed)

مراجعة مفكك Objective-C و Swift Code

في هذا القسم ، سنستكشف الكود الثنائي لتطبيق iOS يدويًا ونجري تحليلًا ثابتًا عليه .يمكن أن يكون التحليل اليدوي عملية بطيئة وتتطلب صبراً هائلاً .يمكن أن يجعل التحليل اليدوي الجيد التحليل الديناميكي أكثر نجاحًا

لا توجد قواعد مكتوبة صارمة لإجراء التحليل الثابت ، ولكن هناك القليل من القواعد العامة التي يمكن استخدامها للحصول على نهج منظم للتحليل اليدوي:

فهم عمل التطبيق قيد التقييم - الهدف من التطبيق وكيف يتصرف في حالة الإدخال الخاطئ.

استكشف السلاسل المختلفة الموجودة في التطبيق الثنائي ، يمكن أن يكون هذا مفيدًا للغاية ، على سبيل المثال في اكتشاف الوظائف المثيرة للاهتمام ومنطق معالجة الأخطاء المحتمل في التطبيق.

ابحث عن الوظائف والفئات ذات الأسماء ذات الصلة بهدفنا

أخيرًا ، ابحث عن نقاط الدخول المختلفة في التطبيق وتابع من هناك لاستكشاف التطبيق.

تعتبر الأساليب التي تمت مناقشتها في هذا القسم عامة وقابلة للتطبيق بغض النظر عن الأدوات المستخدمة في التحليل.

ج موضوعية

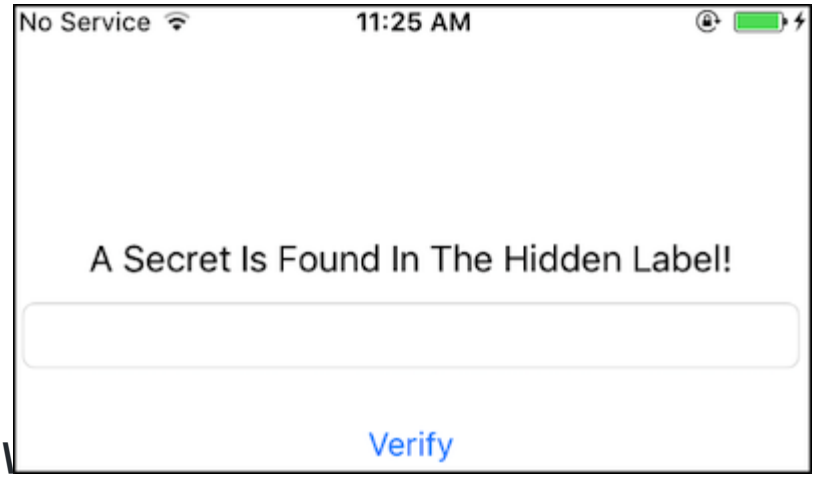
بالإضافة إلى التقنيات التي تم تعلمها في قسم " التفكيك وإلغاء التحويل البرمجي " ، ستحتاج في هذا القسم إلى بعض الفهم لوقت تشغيل . Objective-C على سبيل المثال ، دالات مثل objc_msgSend_أو objc_release_ذات مغزى خاص لوقت تشغيل.Objective-C

وسوف يتم استخدام التطبيق crackme UnCrackable المستوى للجربة ،

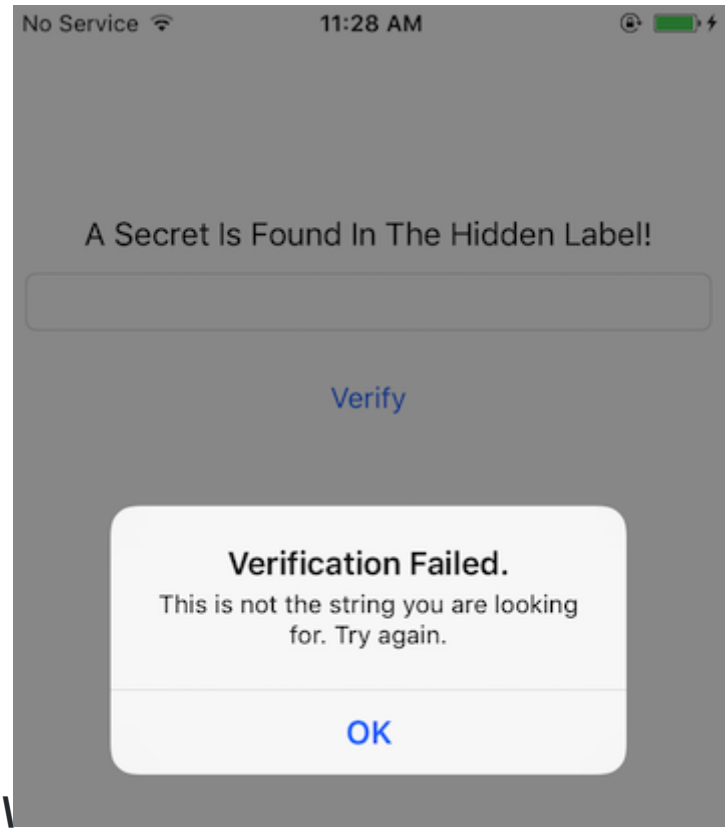
https://github.com/OWASP/owasp-mstg/blob/master/Crackmes/iOS/Level_01/UnCrackable_Level1.ipa

والتي لديها هدف بسيط في العثور على *سلسلة سرية* مخبأة في مكان ما في ثنائي .يحتوي التطبيق على شاشة رئيسية واحدة ويمكن للمستخدم التفاعل عن طريق إدخال سلاسل مخصصة في حقل النص المقدم.

II7MAD99@GMAIL.COM 26 Oct 2021



عندما يقوم المستخدم بإدخال سلسلة خاطئة ، يعرض التطبيق نافذة منبثقة بها رسالة "فشل التحقق."



يمكنك الاحتفاظ بملاحظة السلاسل المعروضة في النافذة المنبثقة ، حيث قد يكون ذلك مفيدًا عند البحث عن الكود حيث تتم معالجة الإدخال ويتم اتخاذ القرار .لحسن الحظ ، فإن التعقيد والتفاعل مع هذا التطبيق واضح ومباشر ، مما يبشر بالخير لمساعينا العكسية.

للتحليل الثابت في هذا القسم ، سنستخدم .Ghidra 9.0.4 تحليل Ghidra 9.1_beta

التلقائي به خطأ ولا يُظهر فئات.Objective-C

II7MAD99@GMAIL.COM 26 Oct 2021

يمكننا أن نبدأ بفحص السلاسل الموجودة في الثنائي عن طريق فتحه في .Ghidra

قد تكون السلاسل المدرجة مربكة في البداية ، ولكن مع بعض الخبرة في عكس كود Objective-C، ستتعلم كيفية *تصفية* وتجاهل السلاسل غير المفيدة أو ذات الصلة حقًا .على سبيل المثال ، تلك الموضحة في لقطة الشاشة أدناه ، والتي تم إنشاؤها لوقت تشغيل .Objective-C قد تكون السلاسل الأخرى مفيدة في بعض الحالات ، مثل تلك التي تحتوي على رموز (أسماء الوظائف وأسماء الفئات وما إلى ذلك) وسنستخدمها عند إجراء تحليل ثابت للتحقق من استخدام بعض الوظائف المحددة.

10000b4b6	@:#	"@:#"	ds
10000b4ba	NSManagedObject	"NSManagedObject"	ds
10000b4ca	NSConstantString	"NSConstantString"	ds
10000b4db	NSString	"NSString"	ds
10000b4e4	NSKnownKeysMappingStrategy1	"NSKnownKeysMappingStrategy1"	ds
10000b500	NSKnownKeysDictionary1	"NSKnownKeysDictionary1"	ds
10000b517	_objc_readClassPair	"_objc_readClassPair"	ds
10000b52b	_objc_allocateClassPair	"_objc_allocateClassPair"	ds
10000b543	_object_getIndexedIvars	"_object_getIndexedIvars"	ds
10000b55b	_objc_getClass	"_objc_getClass"	ds
10000b56a	_objc_getMetaClass	"_objc_getMetaClass"	ds
10000b57d	_objc_getRequiredClass	"_objc_getRequiredClass"	ds
10000b594	_objc_lookUpClass	"_objc_lookUpClass"	ds
10000b5a6	_objc_getProtocol	"_objc_getProtocol"	ds
10000b5b8	_class_getName	"_class_getName"	ds
10000b5c7	_protocol_getName	"_protocol_getName"	ds
10000b5d9	_objc_copyClassNamesForIma...	"_objc_copyClassNamesForImage"	ds
10000b5f6	v@:	"v@:"	ds
10000b5fa	Swift	"Swift"	ds
10000b600	_Tt%cSs%zu%.*s%s	"_Tt%cSs%zu%.*s%s"	ds
10000b611	_	"_"	ds
10000b613	_Tt%c%zu%.*s%zu%.*s%s	"_Tt%c%zu%.*s%zu%.*s%s"	ds
10000b629	_TtP	"_TtP"	ds
10000b62e	_TtC	"_TtC"	ds
10000b633	Ss	"Ss"	ds
10000b636	%.*s.%.*s	"%.*s.%.*s"	ds
10000b640	__TEXT	"__TEXT"	ds
10000b647	__LINKEDIT	"__LINKEDIT"	ds
10000b652	ViewController	"ViewController"	ds

١

إذا واصلنا تحليلنا الدقيق ، فيمكننا تحديد السلسلة ، "فشل التحقق" ، والتي يتم استخدامها في النافذة المنبثقة عند تقديم إدخال خاطئ .إذا اتبعت المراجع التبادلية (Xrefs)لهذه السلسلة ، فستصل إلى buttonClick وظيفة ViewController الفصل .سننظر في buttonClick الوظيفة لاحقًا في هذا القسم .عند إجراء مزيد من التحقق من السلاسل الأخرى في التطبيق ، فإن عددًا قليلاً منها فقط يبدو مرشحًا محتملًا لعلامة *مخفية* .يمكنك تجربتهم والتحقق كذلك.

II7MAD99@GMAIL.COM 26 Oct 2021

Defined Strings - 457 items

Location	String Value	String Representation	Data T...
10000b187	debugDescription	"debugDescription"	ds
10000b198	_window	"_window"	ds
10000b1a0	load	"load"	ds
10000b1a5	setObject:forKeyedSubscript:	"setObject:forKeyedSubscript:"	ds
10000b1c2	setObject:forKey:	"setObject:forKey:"	ds
10000b1d4	removeObjectForKey:	"removeObjectForKey:"	ds
10000b1e8	objectForKeyedSubscript:	"objectForKeyedSubscript:"	ds
10000b201	init	"init"	ds
10000b206	allocWithEntity:	"allocWithEntity:"	ds
10000b217	allocBatch:withEntity:count:	"allocBatch:withEntity:count:"	ds
10000b234	fastIndexForKnownKey:	"fastIndexForKnownKey:"	ds
10000b24a	indexForKey:	"indexForKey:"	ds
10000b257	objectForKey:	"objectForKey:"	ds
10000b265	addEntriesFromDictionary:	"addEntriesFromDictionary:"	ds
10000b27f	initialize	"initialize"	ds
10000b28a	lengthOfBytesUsingEncoding:	"lengthOfBytesUsingEncoding:"	ds
10000b2a6	getCString:maxLength:enco...	"getCString:maxLength:encoding:"	ds
10000b2c5	initWithBytes:length:encoding:	"initWithBytes:length:encoding:"	ds
10000b2e4	keyEnumerator	"keyEnumerator"	ds
10000b2f2	nextObject	"nextObject"	ds
10000b2fd	Congratulations!	"Congratulations!"	ds
10000b30e	You found the secret!!	"You found the secret!!"	ds
10000b325	OK	"OK"	ds
10000b328	Verification Failed.	"Verification Failed."	ds
10000b33d	This is not the string you ar...	"This is not the string you are looking for. Try agai...	ds
10000b374	theLabel	"theLabel"	ds
10000b37d	T@"UILabel",W,N,V_theLabel	"T@\"UILabel\",W,N,V_theLabel"	ds
10000b398	Hint	"Hint"	ds
10000b39d	T@"UILabel",W,N,V_Hint	"T@\"UILabel\",W,N,V_Hint"	ds
10000b3b4	theTextField	"theTextField"	ds
10000b3c1	T@"UITextField",W,N,V_theT...	"T@\"UITextField\",W,N,V_theTextField"	ds
10000b3e4	bVerify	"bVerify"	ds
10000b3ec	T@"UIButton",W,N,V_bVerify	"T@\"UIButton\",W,N,V_bVerify"	ds
10000b407	hash	"hash"	ds

١

للمضي قدمًا ، لدينا طريقان يجب أن نسلكهما .إما أن نبدأ في تحليل buttonClickالوظيفة المحددة في الخطوة أعلاه ، أو نبدأ في تحليل التطبيق من نقاط الدخول المختلفة .في وضع العالم الحقيقي ، في معظم الأوقات سوف تسلك المسار الأول ، ولكن من منظور التعلم ، في هذا القسم ، سنتخذ المسار الأخير.

يستدعي تطبيق iOS وظائف مختلفة محددة مسبقًا يوفرها وقت تشغيل iOS اعتمادًا على حالته داخل دورة حياة التطبيق . تُعرف هذه الوظائف بنقاط دخول التطبيق .فمثلا:

[AppDelegate application:didFinishLaunchingWithOptions:]

عند بدء تشغيل التطبيق لأول مرة

[AppDelegate applicationDidBecomeActive:]

يتم استدعاء عندما ينتقل التطبيق من حالة غير نشطة إلى حالة نشطة

تقوم العديد من التطبيقات بتنفيذ التعليمات البرمجية الهامة في هذه الأقسام ، وبالتالي فهي عادةً نقطة انطلاق جيدة لاتباع الكود بشكل منهجي.

II7MAD99@GMAIL.COM 26 Oct 2021

بمجرد الانتهاء من تحليل جميع الوظائف في AppDelegate الفصل ، يمكننا أن نستنتج أنه لا يوجد رمز ذي صلة موجود .يثير عدم وجود أي رمز في الوظائف المذكورة أعلاه السؤال - من أين يتم استدعاء رمز التهيئة للتطبيق؟

لحسن الحظ ، يحتوي التطبيق الحالي على قاعدة رمز صغيرة ، ويمكننا العثور على ViewControllerفئة أخرى في عرض Symbol Tree

في هذه الفئة ، viewDidLoad تبدو وظيفة الوظيفة مثيرة للاهتمام .إذا قمت بالتحقق من وثائق viewDidLoad، يمكنك أن ترى أنه يمكن أيضًا استخدامها لإجراء تهيئة إضافية على طرق العرض

Decompile: viewDidLoad - (uncrackable.arm64)

```
1
2  /* Function Stack Size: 0x10 bytes */
3
4  void viewDidLoad(ID param_1,SEL param_2)
5
6  {
7    undefined8 uVar1;
8    undefined8 uVar2;
9    ID local_40;
10   class_t *local_38;
11
12   local_38 = &ViewController;
13   local_40 = param_1;
14   _objc_msgSendSuper2(&local_40,"viewDidLoad");
15   Hint(param_1,(SEL)"Hint");
16   uVar1 = _objc_retainAutoreleasedReturnValue();
17   _objc_msgSend(uVar1,"setNumberOfLines:",1);
18   _objc_release(uVar1);
19   Hint(param_1,(SEL)"Hint");
20   uVar1 = _objc_retainAutoreleasedReturnValue();
21   _objc_msgSend(uVar1,"setAdjustsFontSizeToFitWidth:",1);
22   _objc_release(uVar1);
23   Hint(param_1,(SEL)"Hint");
24   uVar1 = _objc_retainAutoreleasedReturnValue();
25   _objc_msgSend(uVar1,"sizeToFit");
26   _objc_release(uVar1);
27   theLabel(param_1,(SEL)"theLabel");
28   uVar1 = _objc_retainAutoreleasedReturnValue();
29   _objc_msgSend(uVar1,"setHidden:",1);
30   _objc_release(uVar1);
31   uVar1 = FUN_1000080d4();
32   _objc_msgSend(&_OBJC_CLASS_$_NSString,"stringWithCString:encoding:",uVar1,1);
33   uVar1 = _objc_retainAutoreleasedReturnValue();
34   theLabel(param_1,(SEL)"theLabel");
35   uVar2 = _objc_retainAutoreleasedReturnValue();
36   _objc_msgSend(uVar2,"setText:",uVar1);
37   _objc_release(uVar2);
38   _objc_release(uVar1);
39   return;
40 }
41
```

Label text being set

II7MAD99@GMAIL.COM 26 Oct 2021

على .إذا تحققنا من إلغاء ترجمة هذه الوظيفة ، فهناك بعض الأشياء المثيرة للاهتمام التي تحدث
سبيل المثال ، هناك استدعاء لوظيفة أصلية في السطر ٣١ ويتم تهيئة التسمية
يمكنك الاحتفاظ بملاحظة هذه .بعلامة مضبوطة على ١ في السطور ٢٧-٢٩setHidden
الملاحظات ومتابعة استكشاف الوظائف الأخرى في هذا الفصل للإيجاز ، يتم ترك استكشاف الأجزاء
.الأخرى من الوظيفة كتدريب للقراء
في خطوتنا الأولى ، لاحظنا أن التطبيق يتحقق من سلسلة الإدخال فقط عند الضغط على زر واجهة
كما ذكرنا سابقًا ، تحتوي .الوظيفة هدفًا واضحًاbuttonClickوبالتالي ، يعد تحليل .المستخدم
في السطر ٢٩ ، يتم اتخاذ قرار .هذه الوظيفة أيضًا على السلسلة التي نراها في النوافذ المنبثقة
يأتي إدخال (السطر ٢٣uVar1 تم حفظ المخرجات في)isEqualString يستند إلى نتيجة
لذلك ، يمكننا أن نفترض أن العلامة .labelالمقارنة من حقل إدخال النص (من المستخدم) وقيمة
.المخفية مخزنة في تلك التسمية

Decompile: buttonClick: - (uncrackable.arm64)

```
1
2  /* Function Stack Size: 0x18 bytes */
3
4  void buttonClick:(ID param_1,SEL param_2,ID param_3)
5
6  {
7    int iVar1;
8    undefined8 uVar2;
9    undefined8 uVar3;
10   undefined8 uVar4;
11   undefined8 uVar5;
12   cfstringStruct *pcVar6;
13   cfstringStruct *pcVar7;
14
15   theTextField(param_1,(SEL)"theTextField");
16   uVar2 = _objc_retainAutoreleasedReturnValue();
17   _objc_msgSend(uVar2,"text");
18   uVar3 = _objc_retainAutoreleasedReturnValue();
19   theLabel(param_1,(SEL)"theLabel");
20   uVar4 = _objc_retainAutoreleasedReturnValue();
21   _objc_msgSend(uVar4,"text");
22   uVar5 = _objc_retainAutoreleasedReturnValue();
23   iVar1 = _objc_msgSend(uVar3,"isEqualToString:",uVar5);
24   _objc_release(uVar5);
25   _objc_release(uVar4);
26   _objc_release(uVar3);
27   _objc_release(uVar2);
28   uVar2 = _objc_msgSend(&_OBJC_CLASS_$_UIAlertView,"alloc");
29   if (iVar1 == 0) {                                  Decision based on uVar1 value
30     pcVar6 = &cf_VerificationFailed.;
31     pcVar7 = &cf_Thisisnotthestringyouarelookingfor.Tryagain.;
32   }
33   else {
34     pcVar6 = &cf_Congratulations!;
35     pcVar7 = &cf_Youfoundthesecret!!;
36   }
37   uVar2 = _objc_msgSend(uVar2,"initWithTitle:message:delegate:cancelButtonTitle:otherButtonTi
38                         pcVar6,pcVar7,param_1,&cf_OK,0);
39   _objc_msgSend(uVar2,"show");
40   _objc_release(uVar2);
41   return;
42 }
43
```

\

II7MAD99@GMAIL.COM 26 Oct 2021

خلصنا أيضًا إلى .الآن تابعنا التدفق الكامل ولدينا جميع المعلومات حول تدفق التطبيق أن العلامة المخفية موجودة في تسمية نصية ومن أجل تحديد قيمة التسمية ، نحتاج الوظيفة ، وفهم ما يحدث في الوظيفة الأصلية viewDidLoad

Decompile: viewDidLoad - (uncrackable.arm64)

```
1
2  /* Function Stack Size: 0x10 bytes */
3
4  void viewDidLoad(ID param_1,SEL param_2)
5
6  {
7    undefined8 uVar1;
8    undefined8 uVar2;
9    ID local_40;
10   class_t *local_38;
11
12   local_38 = &ViewController;
13   local_40 = param_1;
14   _objc_msgSendSuper2(&local_40,"viewDidLoad");
15   Hint(param_1,(SEL)"Hint");
16   uVar1 = _objc_retainAutoreleasedReturnValue();
17   _objc_msgSend(uVar1,"setNumberOfLines:",1);
18   _objc_release(uVar1);
19   Hint(param_1,(SEL)"Hint");
20   uVar1 = _objc_retainAutoreleasedReturnValue();
21   _objc_msgSend(uVar1,"setAdjustsFontSizeToFitWidth:",1);
22   _objc_release(uVar1);
23   Hint(param_1,(SEL)"Hint");
24   uVar1 = _objc_retainAutoreleasedReturnValue();
25   _objc_msgSend(uVar1,"sizeToFit");
26   _objc_release(uVar1);
27   theLabel(param_1,(SEL)"theLabel");
28   uVar1 = _objc_retainAutoreleasedReturnValue();
29   _objc_msgSend(uVar1,"setHidden:",1);
30   _objc_release(uVar1);
31   uVar1 = FUN_1000080d4();
32   _objc_msgSend(&_OBJC_CLASS_$_NSString,"stringWithCString:encoding:",uVar1,1);
33   uVar1 = _objc_retainAutoreleasedReturnValue();
34   theLabel(param_1,(SEL)"theLabel");
35   uVar2 = _objc_retainAutoreleasedReturnValue();
36   _objc_msgSend(uVar2,"setText:",uVar1);
37   _objc_release(uVar2);
38   _objc_release(uVar1);
39   return;
40 }
41
```

Label text being set

١

إذا تحققنا من إلغاء ترجمة هذه الوظيفة ، فهناك بعض الأشياء المثيرة للاهتمام التي تحدث .على سبيل المثال ، هناك استدعاء لوظيفة أصلية في السطر ٣١ ويتم تهيئة التسمية setHidden بعلامة مضبوطة على ١ في السطور ٢٧-٢٩ .يمكنك الاحتفاظ

II7MAD99@GMAIL.COM 26 Oct 2021

بملاحظة هذه الملاحظات ومتابعة استكشاف الوظائف الأخرى في هذا الفصل .للإيجاز ، يتم ترك استكشاف الأجزاء الأخرى من الوظيفة كتدريب للقراء.

في خطوتنا الأولى ، لاحظنا أن التطبيق يتحقق من سلسلة الإدخال فقط عند الضغط على زر واجهة المستخدم .وبالتالي ، يعد تحليل buttonClickالوظيفة هدفًا واضحًا .كما ذكرنا سابقًا ، تحتوي هذه الوظيفة أيضًا على السلسلة التي نراها في النوافذ المنبثقة .في السطر ٢٩ ، يتم اتخاذ قرار يستند إلى نتيجة)isEqualString تم حفظ المخرجات في uVar1 السطر ٢٣ (يأتي إدخال المقارنة من حقل إدخال النص (من المستخدم) وقيمة .label لذلك ، يمكننا أن نفترض أن العلامة المخفية مخزنة في تلك التسمية

Decompile: buttonClick: - (uncrackable.arm64)

```
1
2  /* Function Stack Size: 0x18 bytes */
3
4  void buttonClick:(ID param_1,SEL param_2,ID param_3)
5
6  {
7    int iVar1;
8    undefined8 uVar2;
9    undefined8 uVar3;
10   undefined8 uVar4;
11   undefined8 uVar5;
12   cfstringStruct *pcVar6;
13   cfstringStruct *pcVar7;
14
15   theTextField(param_1,(SEL)"theTextField");
16   uVar2 = _objc_retainAutoreleasedReturnValue();
17   _objc_msgSend(uVar2,"text");
18   uVar3 = _objc_retainAutoreleasedReturnValue();
19   theLabel(param_1,(SEL)"theLabel");
20   uVar4 = _objc_retainAutoreleasedReturnValue();
21   _objc_msgSend(uVar4,"text");
22   uVar5 = _objc_retainAutoreleasedReturnValue();
23   iVar1 = _objc_msgSend(uVar3,"isEqualToString:",uVar5);
24   _objc_release(uVar5);
25   _objc_release(uVar4);
26   _objc_release(uVar3);
27   _objc_release(uVar2);
28   uVar2 = _objc_msgSend(&_OBJC_CLASS_$_UIAlertView,"alloc");
29   if (iVar1 == 0) {                                  Decision based on uVar1 value
30     pcVar6 = &cf_VerificationFailed.;
31     pcVar7 = &cf_Thisisnotthestringyouarelookingfor.Tryagain.;
32   }
33   else {
34     pcVar6 = &cf_Congratulations!;
35     pcVar7 = &cf_Youfoundthesecret!!;
36   }
37   uVar2 = _objc_msgSend(uVar2,"initWithTitle:message:delegate:cancelButtonTitle:otherButtonTi
38                         pcVar6,pcVar7,param_1,&cf_OK,0);
39   _objc_msgSend(uVar2,"show");
40   _objc_release(uVar2);
41   return;
42 }
43
```

الآن تابعنا التدفق الكامل ولدينا جميع المعلومات حول تدفق التطبيق .خلصنا أيضًا إلى أن العلامة المخفية موجودة في تسمية نصية ومن أجل تحديد قيمة التسمية ، نحتاج إلى إعادة النظر في viewDidLoad الوظيفة ، وفهم ما يحدث في الوظيفة الأصلية المحددة

يتطلب تحليل الكود الأصلي المفكك فهمًا جيدًا لاتفاقيات الاستدعاء والتعليمات المستخدمة بواسطة النظام الأساسي

II7MAD99@GMAIL.COM 26 Oct 2021

في جميع أنحاء الدليل ، نستخدم "اختبار أمان تطبيقات الأجهزة المحمولة" ككلمة شاملة للإشارة إلى تقييم أمان تطبيقات الأجهزة المحمولة عبر التحليل الثابت والديناميكي .تُستخدم مصطلحات مثل "اختبار اختراق تطبيقات الأجهزة المحمولة" و "مراجعة أمان تطبيقات الأجهزة المحمولة" بشكل غير متسق إلى حد ما في صناعة الأمان ، ولكن تشير هذه المصطلحات إلى نفس الشيء تقريبًا .عادةً ما يكون اختبار أمان تطبيقات الأجهزة المحمولة جزءًا من تقييم أمني أكبر أو اختبار اختراق يشتمل على بنية خادم العميل وواجهات برمجة التطبيقات من جانب الخادم التي يستخدمها تطبيق الأجهزة المحمولة.

في هذا الدليل ، نغطي اختبار أمان تطبيقات الأجهزة المحمولة في سياقين .الأول هو اختبار الأمان "الكلاسيكي" الذي اكتمل قرب نهاية دورة حياة التطوير .في هذا السياق ، يصل المُختبِر إلى إصدار شبه مكتمل أو جاهز للإنتاج من التطبيق ، ويحدد مشكلات الأمان ، ويكتب تقريرًا (عادةً ما يكون مدمرًا) .يتميز السياق الآخر بتنفيذ المتطلبات وأتمتة اختبارات الأمان من بداية دورة حياة تطوير البرمجيات فصاعدًا .تنطبق نفس المتطلبات الأساسية وحالات الاختبار على كلا السياقين ، ولكن تختلف الطريقة عالية المستوى ومستوى تفاعل العميل.

مبادئ الاختبار

اختبار الصندوق الأبيض مقابل اختبار الصندوق الأسود

لنبدأ بتحديد المفاهيم:

- يتم إجراء اختبار الصندوق الأسود دون أن يكون لدى المختبر أي معلومات حول التطبيق قيد الاختبار .تسمى هذه العملية أحيانًا "اختبار المعرفة الصفرية ."الغرض الرئيسي من هذا الاختبار هو السماح للمختبِر بالتصرف كمهاجم حقيقي بمعنى استكشاف الاستخدامات الممكنة للمعلومات المتاحة للجمهور والقابلة للاكتشاف
- اختبار الصندوق الأبيض (يسمى أحيانًا "اختبار المعرفة الكاملة") هو عكس اختبار الصندوق الأسود تمامًا ، بمعنى أن المختبِر لديه معرفة كاملة بالتطبيق .قد تشمل المعرفة الكود المصدري والوثائق والمخططات .يسمح هذا النهج باختبار أسرع بكثير من اختبار الصندوق الأسود نظرًا لشفافيته ومع المعرفة الإضافية المكتسبة ، يمكن للمختبِر إنشاء حالات اختبار أكثر تعقيدًا وحبيبية.
- اختبار الصندوق الرمادي هو جميع الاختبارات التي تقع بين نوعي الاختبار المذكورين أعلاه: يتم تقديم بعض المعلومات للمختبِر (عادةً ما تكون بيانات الاعتماد فقط) ، ومن المقرر اكتشاف معلومات أخرى .هذا النوع من الاختبارات

II7MAD99@GMAIL.COM 26 Oct 2021

هو حل وسط مثير للاهتمام في عدد حالات الاختبار والتكلفة والسرعة ونطاق الاختبار .اختبار الصندوق الرمادي هو أكثر أنواع الاختبارات شيوعًا في صناعة الأمان.

ننصح بشدة أن تطلب شفرة المصدر حتى تتمكن من استخدام وقت الاختبار بأكبر قدر ممكن من الكفاءة .من الواضح أن الوصول إلى الكود الخاص بالمختبر لا يحاكي هجومًا خارجيًا ، لكنه يبسط تحديد الثغرات الأمنية من خلال السماح للمختبِر بالتحقق من كل حالة شاذة أو سلوك مشبوه تم تحديده على مستوى الكود .اختبار المربع الأبيض هو السبيل للذهاب إذا لم يتم اختبار التطبيق من قبل.

على الرغم من أن إلغاء التحويل البرمجي على نظام Android أمر بسيط ، إلا أن شفرة المصدر قد تكون غامضة ، وسيستغرق إلغاء التعتيم وقتًا طويلاً .ولذلك فإن قيود الوقت هي سبب آخر للمختبِر للوصول إلى الكود المصدري.

تحليل الضعف

عادةً ما يكون تحليل الثغرات هو عملية البحث عن الثغرات الأمنية في التطبيق .على الرغم من إمكانية القيام بذلك يدويًا ، إلا أن الماسحات الآلية تُستخدم عادةً لتحديد نقاط الضعف الرئيسية .التحليل الساكن والديناميكي هما نوعان من تحليل نقاط الضعف.

التحليل الثابت مقابل التحليل الديناميكي

يتضمن اختبار أمان التطبيق الثابت (SAST) فحص مكونات التطبيق دون تنفيذها ، من خلال تحليل كود المصدر إما يدويًا أو تلقائيًا .يوفر OWASP معلومات حول تحليل الكود الثابت التي قد تساعدك على فهم التقنيات ونقاط القوة والضعف والقيود.

يتضمن اختبار أمان التطبيق الديناميكي (DAST) فحص التطبيق أثناء وقت التشغيل .يمكن أن يكون هذا النوع من التحليل يدويًا أو تلقائيًا .لا يوفر عادةً المعلومات التي يوفرها التحليل الثابت ، ولكنه طريقة جيدة لاكتشاف العناصر المثيرة للاهتمام (الأصول والميزات ونقاط الدخول وما إلى ذلك) من وجهة نظر المستخدم.

الآن بعد أن حددنا التحليل الثابت والديناميكي ، دعنا نتعمق أكثر.

التحليل الساكن

أثناء التحليل الثابت ، تتم مراجعة الكود المصدري لتطبيق الهاتف المحمول لضمان التنفيذ المناسب لضوابط الأمان .في معظم الحالات ، يتم استخدام نهج أوتوماتيكي / يدوي مختلط .تلتقط عمليات المسح التلقائي الفاكهة المنخفضة المعلقة ، ويمكن للمختبِر البشري استكشاف قاعدة الشفرة مع وضع سياقات استخدام محددة في الاعتبار.

II7MAD99@GMAIL.COM 26 Oct 2021

مراجعة التعليمات البرمجية اليدوية

يقوم أحد المختبرين بمراجعة الكود يدويًا عن طريق التحليل اليدوي للكود المصدري لتطبيق الهاتف المحمول بحثًا عن الثغرات الأمنية .تتراوح الطرق من البحث الأساسي بالكلمة الرئيسية عبر الأمر "grep" إلى فحص التعليمات البرمجية المصدر سطريًا .غالبًا ما توفر بيئات التطوير المتكاملة (IDEs) وظائف مراجعة التعليمات البرمجية الأساسية ويمكن توسيعها باستخدام أدوات متنوعة.

يستلزم النهج الشائع لتحليل الكود اليدوي تحديد مؤشرات الضعف الأمنية الرئيسية من خلال البحث عن واجهات برمجة تطبيقات وكلمات رئيسية معينة ، مثل استدعاءات الطريقة المتعلقة بقاعدة البيانات مثل "executeStatement" أو "executeQuery".الكود الذي يحتوي على هذه السلاسل هو نقطة انطلاق جيدة للتحليل اليدوي.

على عكس التحليل التلقائي للكود ، تعد المراجعة اليدوية للكود جيدة جدًا لتحديد نقاط الضعف في منطق الأعمال ، وانتهاكات المعايير ، وعيوب التصميم ، خاصةً عندما تكون الشفرة آمنة تقنيًا ولكنها معيبة منطقيًا .من غير المحتمل أن يتم اكتشاف مثل هذه السيناريوهات بواسطة أي أداة تحليل شفرة تلقائية.

تتطلب المراجعة اليدوية للكود مراجعًا خبيرًا للكود يتقن كل من اللغة والأطر المستخدمة في تطبيق الهاتف المحمول .يمكن أن تكون المراجعة الكاملة للكود عملية بطيئة ومملة وتستغرق وقتًا طويلاً بالنسبة للمراجع ، خاصةً بالنظر إلى قواعد التعليمات البرمجية الكبيرة مع العديد من التبعيات.

تحليل كود المصدر الآلي

يمكن استخدام أدوات التحليل الآلي لتسريع عملية مراجعة اختبار أمان التطبيقات الثابتة (SAST).يقومون بالتحقق من كود المصدر للامتثال لمجموعة محددة مسبقًا من القواعد أو أفضل ممارسات الصناعة ، ثم يعرضون عادةً قائمة بالنتائج أو التحذيرات والعلامات لجميع الانتهاكات المكتشفة .تعمل بعض أدوات التحليل الثابت مقابل التطبيق المترجم فقط ، ويجب تغذية بعضها برمز المصدر الأصلي ، بينما يعمل البعض الآخر كمكونات إضافية للتحليل المباشر في بيئة التطوير المتكاملة.(IDE)

على الرغم من أن بعض أدوات تحليل الكود الثابت تتضمن الكثير من المعلومات حول القواعد والدلالات المطلوبة لتحليل تطبيقات الأجهزة المحمولة ، إلا أنها قد تنتج العديد من الإيجابيات الخاطئة ، خاصةً إذا لم يتم تكوينها للبيئة المستهدفة .لذلك يجب على أخصائي الأمن مراجعة النتائج دائمًا.

يتضمن ملحق "أدوات الاختبار" قائمة بأدوات التحليل الثابتة ، والتي يمكن العثور عليها في نهاية هذا الكتاب.

II7MAD99@GMAIL.COM 26 Oct 2021

التحليل الديناميكي

ينصب تركيز DAST على اختبار وتقييم التطبيقات من خلال تنفيذها في الوقت الفعلي .الهدف الرئيسي للتحليل الديناميكي هو اكتشاف الثغرات الأمنية أو نقاط الضعف في البرنامج أثناء تشغيله .يتم إجراء التحليل الديناميكي على كل من طبقة النظام الأساسي للجوال وضد خدمات الواجهة الخلفية وواجهات برمجة التطبيقات ، حيث يمكن تحليل أنماط الطلب والاستجابة لتطبيق الهاتف المحمول.

يستخدم التحليل الديناميكي عادةً للتحقق من آليات الأمان التي توفر حماية كافية ضد أكثر أنواع الهجمات انتشارًا ، مثل الكشف عن البيانات أثناء النقل ، ومشكلات المصادقة والترخيص ، وأخطاء تكوين الخادم.

تجنب الإيجابيات الكاذبة

أدوات المسح الآلي

يمثل افتقار أدوات الاختبار الآلي حساسية لسياق التطبيق تحديًا .قد تحدد هذه الأدوات مشكلة محتملة لا صلة لها بالموضوع .تسمى هذه النتائج "الإيجابيات الكاذبة."

على سبيل المثال ، يقوم مختبرو الأمان بالإبلاغ عن نقاط الضعف التي يمكن استغلالها في متصفح الويب ولكنها ليست ذات صلة بتطبيق الهاتف .يحدث هذا الخطأ الإيجابي لأن الأدوات الآلية المستخدمة لفحص خدمة الواجهة الخلفية تستند إلى تطبيقات الويب العادية المستندة إلى المستعرض .يتم الإبلاغ عن مشكلات مثل CSRF (تزوير الطلبات عبر المواقع) والبرمجة عبر المواقع (XSS) وفقًا لذلك.

لنأخذ CSRF كمثال .يتطلب هجوم CSRF الناجح ما يلي:

- القدرة على جذب المستخدم الذي قام بتسجيل الدخول لفتح ارتباط ضار في متصفح الويب المستخدم للوصول إلى الموقع المعرض للخطر.
- يجب أن يضيف العميل (المستعرض) تلقائيًا ملف تعريف ارتباط الجلسة أو رمز مصادقة آخر إلى الطلب.

لا تفي تطبيقات الأجهزة المحمولة بهذه المتطلبات: حتى إذا تم استخدام WebViews وإدارة الجلسة المستندة إلى ملفات تعريف الارتباط ، فإن أي رابط ضار ينقر عليه المستخدم يفتح في المتصفح الافتراضي ، الذي يحتوي على متجر منفصل لملفات تعريف الارتباط.

II7MAD99@GMAIL.COM 26 Oct 2021

يمكن أن تكون البرمجة النصية عبر المواقع المخزنة (XSS) مشكلة إذا كان التطبيق يتضمن WebViews ، وقد يؤدي إلى تنفيذ الأمر إذا كان التطبيق يصدر واجهات JavaScript.ومع ذلك ، نادرًا ما تكون البرمجة النصية عبر المواقع المنعكسة مشكلة للسبب المذكور أعلاه (على الرغم من أن ما إذا كان يجب أن تكون موجودة على الإطلاق أمر قابل للجدل ، فإن الهروب من الإخراج هو ببساطة أفضل ممارسة).

في أي حال ، ضع في اعتبارك سيناريوهات الاستغلال عند إجراء تقييم المخاطر ؛ لا تثق بشكل أعمى في إخراج أداة المسح.

الحافظة

عند كتابة البيانات في حقول الإدخال ، يمكن استخدام الحافظة لنسخ البيانات .يمكن الوصول إلى الحافظة على مستوى النظام وبالتالي يتم مشاركتها بواسطة التطبيقات .يمكن إساءة استخدام هذه المشاركة بواسطة التطبيقات الضارة للحصول على بيانات حساسة تم تخزينها في الحافظة.

قبل نظام التشغيلiOS 9 ، قد يراقب تطبيق ضار لوحة اللصق في الخلفية أثناء الاسترداد بشكل دوري [UIPasteboard generalPasteboard].string.اعتبارًا من نظام التشغيلiOS 9 ، يمكن الوصول إلى محتوى لوحة اللصق للتطبيقات الموجودة في المقدمة فقط ، مما يقلل من سطح هجوم استنشاق كلمات المرور من الحافظة بشكل كبير.
بالنسبة لنظام Android، تم إصدار ثغرة PoC من أجل إظهار متجه الهجوم إذا تم تخزين كلمات المرور داخل الحافظة .كان تعطيل اللصق في حقول إدخال كلمات المرور أحد المتطلبات فيMASVS 1.0 ، ولكن تمت إزالته لعدة أسباب:

- لا يمنع منع اللصق في حقول الإدخال الخاصة بالتطبيق من قيام المستخدم بنسخ المعلومات الحساسة على أي حال .نظرًا لأنه تم نسخ المعلومات بالفعل قبل أن يلاحظ المستخدم أنه لا يمكن لصقها ، فقد قام أحد التطبيقات الضارة بالفعل باستنشاق الحافظة.
- إذا تم تعطيل اللصق في حقول كلمة المرور ، فقد يختار المستخدمون كلمات مرور أضعف يمكنهم تذكرها ولا يمكنهم استخدام مديري كلمات المرور بعد الآن ، مما يتعارض مع الهدف الأصلي المتمثل في جعل التطبيق أكثر أمانًا.

عند استخدام أحد التطبيقات ، يجب أن تظل مدركًا أن التطبيقات الأخرى تقرأ الحافظة باستمرار ، كما فعل تطبيق Facebook . ومع ذلك ، فإن نسخ كلمات المرور يمثل مخاطرة أمنية يجب أن تكون على دراية بها ، ولكن لا يمكن حلها أيضًا عن طريق التطبيق

II7MAD99@GMAIL.COM 26 Oct 2021

اختبار الاختراق المعروف أيضًا باسم Pentesting

يتضمن الأسلوب الكلاسيكي اختبار أمان شامل للبنية النهائية أو شبه النهائية للتطبيق ، على سبيل المثال ، الإصدار المتاح في نهاية عملية التطوير .للاختبار في نهاية عملية التطوير ، نوصي

بمعيار التحقق من أمان تطبيقات الأجهزة المحمولة (MASVS)

وقائمة التحقق المرتبطة بها كخط أساس للاختبار .يتم تنظيم اختبار الأمان النموذجي على النحو التالي:

- الإعداد -تحديد نطاق اختبار الأمان ، بما في ذلك تحديد ضوابط الأمان المعمول بها ، وأهداف اختبار المؤسسة ، والبيانات الحساسة .بشكل عام ، يشمل الإعداد جميع عمليات المزامنة مع العميل بالإضافة إلى الحماية القانونية للمختبِر (الذي غالبًا ما يكون طرفًا ثالثًا) .تذكر أن مهاجمة نظام بدون إذن كتابي أمر غير قانوني في أجزاء كثيرة من العالم!
- الاستخبارات اللقاء -تحليل البيئي و المعماري سياق التطبيق للحصول على فهم السياقية العام.
- رسم خرائط التطبيق بناءً على معلومات من المراحل السابقة ؛ يمكن استكماله بالمسح الآلي واستكشاف التطبيق يدويًا .يوفر التعيين فهماً شاملاً للتطبيق ونقاط دخوله والبيانات التي يحتفظ بها ونقاط الضعف المحتملة الرئيسية .يمكن بعد ذلك تصنيف نقاط الضعف هذه وفقًا للضرر الذي قد يسببه استغلالها بحيث يمكن لمختبِر الأمان تحديد أولوياتها .تتضمن هذه المرحلة إنشاء حالات اختبار يمكن استخدامها أثناء تنفيذ الاختبار.
- الاستغلال -في هذه المرحلة ، يحاول مختبِر الأمان اختراق التطبيق من خلال استغلال الثغرات الأمنية التي تم تحديدها خلال المرحلة السابقة .هذه المرحلة ضرورية لتحديد ما إذا كانت نقاط الضعف هي نقاط ضعف حقيقية وحقيقية.
- الإبلاغ -في هذه المرحلة ، وهو أمر ضروري للعميل ، يقوم اختبار الأمان بالإبلاغ عن الثغرات الأمنية .يتضمن ذلك عملية الاستغلال بالتفصيل ، ويصنف نوع الثغرة الأمنية ، ويوثق المخاطر إذا كان المهاجم قادرًا على اختراق الهدف ويحدد البيانات التي تمكن المختبِر من الوصول إليها بشكل غير قانوني.

تحضير

يجب تحديد مستوى الأمان الذي سيتم اختبار التطبيق عنده قبل الاختبار .يجب تحديد المتطلبات الأمنية في بداية المشروع .لدى المؤسسات المختلفة احتياجات وموارد أمنية مختلفة متاحة للاستثمار في أنشطة الاختبار .على الرغم من أن عناصر التحكم في MASVSالمستوى ١ (L1) قابلة للتطبيق على جميع تطبيقات الأجهزة المحمولة ،

II7MAD99@GMAIL.COM 26 Oct 2021

فإن السير عبر قائمة التحقق الكاملة لعناصر تحكم L1 والمستوى ٢ MASVS (L2) مع أصحاب المصلحة التقنيين والتجاريين يعد طريقة جيدة لاتخاذ قرار بشأن مستوى تغطية الاختبار.

قد يكون للمنظمات التزامات تنظيمية وقانونية مختلفة في مناطق معينة .حتى إذا كان التطبيق لا يتعامل مع البيانات الحساسة ، فقد تكون بعض متطلبات L2 ذات صلة (بسبب لوائح الصناعة أو القوانين المحلية) .على سبيل المثال ، قد تكون المصادقة الثنائية (2FA)إلزامية لتطبيق مالي ويتم فرضها من قبل البنك المركزي للبلد و / أو السلطات التنظيمية المالية.

يمكن أيضًا مراجعة الأهداف / الضوابط الأمنية المحددة مسبقًا في عملية التطوير أثناء المناقشة مع أصحاب المصلحة .قد تتوافق بعض الضوابط مع ضوابط MASVS ، لكن البعض الآخر قد يكون خاصًا بالمنظمة أو التطبيق.

General Testing Information	
Client Name:	
Test Location:	
Start Date:	
Closing Date:	
Name pf Tester	
Testing Scope	All native functions availalbe within <AppName> App.
Verification Level	After consultation with <Customer> it was decided that only Level 1 requrirements are applicable to <AppName>. The data processed such as account numbers are not sensitive data according to data classsification policy <Policy Name>.Credit card numbers, are not handled directly in the mobile app and only on a 3rd party system. Therefore MASVS L1 offers an appropriate level of protection for <AppName>.

يجب أن توافق جميع الأطراف المعنية على القرارات والنطاق في قائمة التحقق لأن هذه ستحدد الأساس لجميع اختبارات الأمان.

التنسيق مع العميل

يمكن أن يكون إعداد بيئة اختبار العمل مهمة صعبة .على سبيل المثال ، قد تعيق القيود المفروضة على نقاط الوصول اللاسلكية والشبكات الخاصة بالمؤسسة التحليل الديناميكي الذي يتم إجراؤه في مقر العميل .قد تحظر سياسات الشركة استخدام الهواتف الجذر أو أدوات اختبار الشبكة (الأجهزة والبرامج) داخل شبكات المؤسسة .قد تؤدي التطبيقات التي تنفذ اكتشاف الجذر وإجراءات الهندسة العكسية الأخرى إلى زيادة كبيرة في العمل المطلوب لمزيد من التحليل.

يتضمن اختبار الأمان العديد من المهام الغازية ، بما في ذلك مراقبة حركة مرور شبكة تطبيق الهاتف المحمول ومعالجتها ، وفحص ملفات بيانات التطبيق ، وإجراء مكالمات API.قد تعيق عناصر التحكم في الأمان ، مثل تثبيت الشهادة واكتشاف الجذر ، هذه المهام وتبطئ الاختبار بشكل كبير.

II7MAD99@GMAIL.COM 26 Oct 2021

للتغلب على هذه العقبات ، قد ترغب في طلب اثنين من متغيرات بناء التطبيق من فريق التطوير .يجب أن يكون أحد المتغيرات عبارة عن إصدار بحيث يمكنك تحديد ما إذا كانت عناصر التحكم التي تم تنفيذها تعمل بشكل صحيح ولا يمكن تجاوزها بسهولة .يجب أن يكون المتغير الثاني عبارة عن بناء تصحيح تم إلغاء تنشيط بعض عناصر التحكم في الأمان من أجله .يعد اختبار بنائين مختلفين هو الطريقة الأكثر فعالية لتغطية جميع حالات الاختبار.

اعتمادًا على نطاق المهمة ، قد لا يكون هذا النهج ممكنًا .سيساعدك طلب إنشاءات الإنتاج وتصحيح الأخطاء لاختبار المربع الأبيض على إكمال جميع حالات الاختبار وتحديد النضج الأمني للتطبيق بوضوح .قد يفضل العميل أن تركز اختبارات الصندوق الأسود على تطبيق الإنتاج وتقييم فعالية ضوابط الأمان الخاصة به.

يجب مناقشة نطاق كلا النوعين من الاختبارات خلال مرحلة الإعداد .على سبيل المثال ، يجب تحديد ما إذا كان يجب تعديل ضوابط الأمان قبل الاختبار .مواضيع إضافية تناقش أدناه.

تحديد البيانات الحساسة

تختلف تصنيفات المعلومات الحساسة حسب الصناعة والبلد .بالإضافة إلى ذلك ، قد تتخذ المؤسسات وجهة نظر تقييدية للبيانات الحساسة ، وقد يكون لديها سياسة تصنيف البيانات التي تحدد المعلومات الحساسة بوضوح.

هناك ثلاث حالات عامة يمكن من خلالها الوصول إلى البيانات:

- في حالة سكون -البيانات موجودة في ملف أو مخزن بيانات
- قيد الاستخدام -قام أحد التطبيقات بتحميل البيانات في مساحة العنوان الخاصة به
- أثناء النقل -تم تبادل البيانات بين تطبيق الهاتف المحمول ونقطة النهاية أو العمليات المستهلكة على الجهاز ، على سبيل المثال ، أثناء) IPC الاتصال بين العمليات(

قد تعتمد درجة التدقيق المناسبة لكل ولاية على أهمية البيانات واحتمالية الوصول إليها .على سبيل المثال ، قد تكون البيانات المحفوظة في ذاكرة التطبيق أكثر عرضة للخطر من البيانات الموجودة على خوادم الويب للوصول إليها عبر مقالب أساسية لأن المهاجمين من المرجح أن يحصلوا على وصول مادي إلى الأجهزة المحمولة أكثر من خوادم الويب.

في حالة عدم توفر سياسة تصنيف البيانات ، استخدم القائمة التالية من المعلومات التي تعتبر حساسة بشكل عام:

II7MAD99@GMAIL.COM 26 Oct 2021

- معلومات مصادقة المستخدم (بيانات الاعتماد ، وأرقام التعريف الشخصية ، وما إلى ذلك)
- معلومات التعريف الشخصية (PII) التي يمكن إساءة استخدامها لسرقة الهوية: أرقام الضمان الاجتماعي ، وأرقام بطاقات الائتمان ، وأرقام الحسابات المصرفية ، والمعلومات الصحية
- معرفات الجهاز التي قد تحدد هوية الشخص
- البيانات الحساسة للغاية التي قد يؤدي اختراقها إلى الإضرار بالسمعة و / أو التكاليف المالية
- أي بيانات تكون حمايتها التزامًا قانونيًا
- أي بيانات فنية تم إنشاؤها بواسطة التطبيق (أو الأنظمة المرتبطة به) والمستخدمة لحماية البيانات الأخرى أو النظام نفسه (على سبيل المثال ، مفاتيح التشفير).

يجب تحديد تعريف "البيانات الحساسة" قبل بدء الاختبار لأن الكشف عن تسرب البيانات الحساسة بدون تعريف قد يكون مستحيلاً.

جمع المعلومات الاستخباراتية

يتضمن جمع المعلومات جمع المعلومات حول بنية التطبيق ، وحالات استخدام الأعمال التي يقدمها التطبيق ، والسياق الذي يعمل فيه التطبيق .يمكن تصنيف هذه المعلومات على أنها "بيئية" أو "معمارية."

المعلومات البيئية

تتضمن المعلومات البيئية:

- أهداف المنظمة للتطبيق .تعمل الوظيفة على تشكيل تفاعل المستخدمين مع التطبيق وقد تزيد من احتمالية استهداف بعض الأسطح من قبل المهاجمين.
- الصناعة ذات الصلة .قد يكون للصناعات المختلفة ملفات تعريف مخاطر مختلفة.
- أصحاب المصلحة والمستثمرون ؛ فهم المهتمين والمسؤولين عن التطبيق.
- العمليات الداخلية وسير العمل والهياكل التنظيمية .قد تخلق العمليات الداخلية وسير العمل الخاصة بالمنظمة فرصًا لعمليات استغلال منطق الأعمال.

المعلومات المعمارية

تشمل المعلومات المعمارية:

II7MAD99@GMAIL.COM 26 Oct 2021

- تطبيق الهاتف المحمول :كيف يصل التطبيق إلى البيانات ويديرها أثناء العملية ، وكيف يتواصل مع الموارد الأخرى ويدير جلسات المستخدم ، وما إذا كان يكتشف نفسه يعمل على الهواتف التي تم كسر حمايتها أو جذرها ويتفاعل مع هذه المواقف.
- نظام التشغيل :أنظمة التشغيل وإصدارات نظام التشغيل التي يعمل عليها التطبيق)بما في ذلك قيود إصدار Android أو (iOS ، سواء كان من المتوقع تشغيل التطبيق على الأجهزة التي تحتوي على عناصر تحكم في إدارة الأجهزة المحمولة (MDM)، وثغرات أمنية ذات صلة في نظام التشغيل.
- الشبكة :استخدام بروتوكولات النقل الآمنة) على سبيل المثال ، (TLS، واستخدام المفاتيح القوية وخوارزميات التشفير) على سبيل المثال ، (SHA-2 لتأمين تشفير حركة مرور الشبكة ، واستخدام تثبيت الشهادة للتحقق من نقطة النهاية ، وما إلى ذلك.
- الخدمات عن بُعد :الخدمات البعيدة التي يستهلكها التطبيق وما إذا كان اختراقها قد يعرض العميل للخطر.

تعيين التطبيق

بمجرد أن يحصل مُختبِر الأمان على معلومات حول التطبيق وسياقه ، فإن الخطوة التالية هي تعيين بنية التطبيق ومحتواه ، على سبيل المثال ، تحديد نقاط الدخول والميزات والبيانات الخاصة به.

عندما يتم إجراء اختبار الاختراق في نموذج المربع الأبيض أو المربع الرمادي ، فإن أي مستندات من داخل المشروع (مخططات معمارية ، ومواصفات وظيفية ، ورمز ، وما إلى ذلك) قد تسهل العملية إلى حد كبير .في حالة توفر كود المصدر ، يمكن أن يكشف استخدام أدوات SAST عن معلومات قيمة حول الثغرات الأمنية) على سبيل المثال ، حقن .(SQL قد تدعم أدوات DAST اختبار الصندوق الأسود وتفحص التطبيق تلقائيًا: بينما يحتاج المختبِر إلى ساعات أو أيام ، قد يؤدي الماسح الضوئي نفس المهمة في بضع دقائق .ومع ذلك ، من المهم أن تتذكر أن الأدوات التلقائية لها قيود ولن تجد إلا ما تمت برمجتها للعثور عليه .لذلك ، قد يكون التحليل البشري ضروريًا لزيادة النتائج من الأدوات التلقائية (غالبًا ما يكون الحدس مفتاحًا لاختبار الأمان).

تعد نمذجة التهديدات أداة مهمة: عادةً ما تدعم المستندات من ورشة العمل تحديد الكثير من المعلومات التي يحتاجها مختبِر الأمان (نقاط الدخول ، والأصول ، ونقاط الضعف ، والخطورة ، وما إلى ذلك) .يُنصح المختبرين بشدة بمناقشة مدى توفر هذه المستندات مع العميل .يجب أن تكون نمذجة التهديد جزءًا أساسيًا من دورة حياة تطوير البرامج .عادة ما تحدث في المراحل الأولى من المشروع.

II7MAD99@GMAIL.COM 26 Oct 2021

و المبادئ التوجيهية النمذجة التهديد المحدد في OWASP قابلة للتطبيق بشكل عام لتطبيقات الجوال

استغلال

لسوء الحظ ، فإن القيود الزمنية أو المالية تحد من العديد من الآفات إلى تعيين التطبيقات عبر الماسحات الضوئية الآلية (لتحليل نقاط الضعف ، على سبيل المثال) .على الرغم من أن نقاط الضعف التي تم تحديدها خلال المرحلة السابقة قد تكون مثيرة للاهتمام ، إلا أنه يجب تأكيد مدى ملاءمتها فيما يتعلق بخمسة محاور:

- الضرر المحتمل -الضرر الذي يمكن أن ينتج عن استغلال الثغرة الأمنية
- قابلية التكاثر -سهولة استنساخ الهجوم
- القابلية للاستغلال -سهولة تنفيذ الهجوم
- المستخدمون المتأثرون -عدد المستخدمين المتأثرين بالهجوم
- الاكتشاف -سهولة اكتشاف الضعف

رغم كل الصعاب ، قد لا تكون بعض الثغرات قابلة للاستغلال وقد تؤدي إلى تنازلات طفيفة ، إن وجدت .قد تبدو نقاط الضعف الأخرى غير مؤذية للوهلة الأولى ، ولكن يتم تحديدها بخطورة بالغة في ظل ظروف اختبار واقعية .المختبرين الذين يمرون بعناية بمرحلة الاستغلال يدعمون اختبار pentesting من خلال توصيف نقاط الضعف وآثارها.

الإبلاغ

ستكون نتائج اختبار الأمان ذات قيمة للعميل فقط إذا تم توثيقها بوضوح .يجب أن يتضمن تقرير pentest الجيد معلومات مثل ، على سبيل المثال لا الحصر ، ما يلي:

- ملخص تنفيذي
- وصف للنطاق والسياق (على سبيل المثال ، الأنظمة المستهدفة)
- الأساليب المستخدمة
- (pentest مصادر المعلومات) سواء قدمها العميل أو تم اكتشافها أثناء اختبار
- (DREAD النتائج ذات الأولوية) على سبيل المثال ، نقاط الضعف التي تم هيكلتها حسب تصنيف
- نتائج مفصلة
- توصيات لإصلاح كل عيب

تتوفر العديد من قوالب تقارير pentest على الإنترنت Google :صديقك!

II7MAD99@GMAIL.COM 26 Oct 2021

اختبار الأمان وSDLC

على الرغم من أن مبادئ اختبار الأمان لم تتغير بشكل جذري في التاريخ الحديث ، فقد تغيرت تقنيات تطوير البرامج بشكل كبير .في الوقت الذي أدى فيه اعتماد ممارسات Agile على نطاق واسع إلى تسريع تطوير البرامج ، كان على مختبري الأمان أن يصبحوا أسرع وأكثر مرونة مع الاستمرار في تقديم برامج جديرة بالثقة.

يركز القسم التالي على هذا التطور ويصف اختبار الأمان المعاصر.

اختبار الأمان أثناء دورة حياة تطوير البرمجيات

تطوير البرمجيات ليس قديمًا جدًا ، بعد كل شيء ، لذا من السهل ملاحظة نهاية التطوير بدون إطار .لقد عانينا جميعًا من الحاجة إلى الحد الأدنى من مجموعة القواعد للتحكم في العمل مع نمو شفرة المصدر.

في الماضي ، كانت منهجيات "الشلال" هي الأكثر اعتمادًا على نطاق واسع: فتم التطوير بخطوات ذات تسلسل محدد مسبقًا .كانت القدرة على التراجع محدودة بخطوة واحدة ، وكانت عيبًا خطيرًا في منهجيات الشلال .على الرغم من أن لديهم ميزات إيجابية مهمة (توفير البنية ، ومساعدة المختبرين في توضيح المكان المطلوب ، والوضوح وسهولة الفهم ، وما إلى ذلك) ، إلا أن لديهم أيضًا سمات سلبية (إنشاء صوامع ، والبطء ، وفرق متخصصة ، وما إلى ذلك).

مع نضوج تطوير البرمجيات ، زادت المنافسة وأصبح المطورون بحاجة إلى الاستجابة لتغيرات السوق بسرعة أكبر أثناء إنشاء منتجات برمجية بميزانيات أصغر .أصبحت فكرة الهيكل الأقل شائعة ، وتعاونت الفرق الأصغر ، مما أدى إلى كسر الصوامع في جميع أنحاء المنظمة .وُلد مفهوم) "Agile" يعد Scrum و XP و RAD أمثلة معروفة لتطبيقات (Agile ؛ لقد مكنت المزيد من الفرق المستقلة من العمل معًا بشكل أسرع.

لم يكن الأمان في الأصل جزءًا لا يتجزأ من تطوير البرامج .لقد كانت فكرة متأخرة ، تم إجراؤها على مستوى الشبكة من قبل فرق التشغيل التي كان عليها تعويض ضعف أمان البرامج !على الرغم من أن الأمن غير المتكامل كان ممكنًا عندما كانت البرامج موجودة داخل محيط ، فقد أصبح المفهوم قديمًا حيث ظهرت أنواع جديدة من استهلاك البرامج مع تقنيات الويب والجوال وإنترنت الأشياء .في الوقت الحاضر ، يجب توفير الأمان داخل البرنامج لأن تعويض نقاط الضعف غالبًا ما يكون صعبًا للغاية.

سيتم استخدام "SDLC" بالتبادل مع "Secure SDLC" في القسم التالي لمساعدتك على استيعاب فكرة أن الأمان جزء من عمليات تطوير البرامج .وبنفس الروح ، نستخدم اسم DevSecOps للتأكيد على حقيقة أن الأمان جزء من.DevOps

II7MAD99@GMAIL.COM 26 Oct 2021

نظرة عامة علىSDLC

الوصف العام لـSDLC

(Agile تتكون SDLCs دائمًا من نفس الخطوات) العملية الكلية متسلسلة في نموذج الشلال ومتكررة في نموذج :

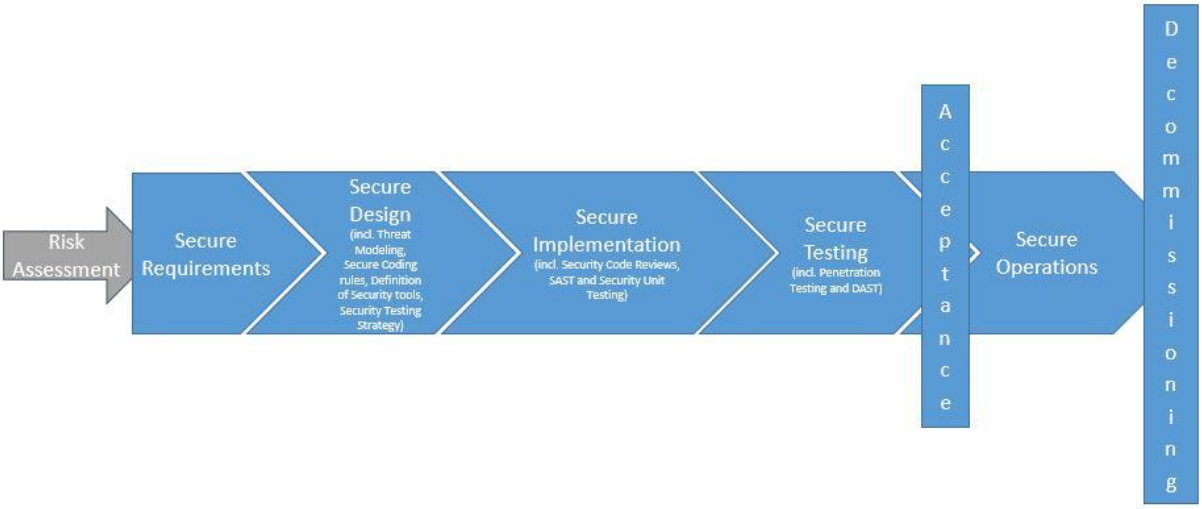
- **قم بإجراء تقييم للمخاطر للتطبيق ومكوناته لتحديد ملفات تعريف المخاطر الخاصة بهم .تعتمد ملفات تعريف المخاطر هذه عادةً على مدى تقبل المؤسسة للمخاطر والمتطلبات التنظيمية المعمول بها .يعتمد تقييم المخاطر أيضًا على عوامل ، بما في ذلك ما إذا كان التطبيق يمكن الوصول إليه عبر الإنترنت ونوع البيانات التي يعالجها التطبيق ويخزنها .يجب أن تؤخذ جميع أنواع المخاطر في الاعتبار: المالية ، والتسويقية ، والصناعية ، وما إلى ذلك. تحدد سياسات تصنيف البيانات البيانات الحساسة وكيف يجب تأمينها.**
- **يتم تحديد متطلبات الأمان في بداية المشروع أو دورة التطوير ، عندما يتم تجميع المتطلبات الوظيفية .تتم إضافة حالات إساءة الاستخدام عند إنشاء حالات الاستخدام .قد تتلقى الفرق (بما في ذلك فرق التطوير) تدريبًا أمنيًا (مثل التشفير الآمن) إذا احتاجوا إليه .يمكنك استخدام OWASP MASVS لتحديد متطلبات الأمان لتطبيقات الهاتف المحمول على أساس مرحلة تقييم المخاطر .تعد مراجعة المتطلبات بشكل متكرر عند إضافة الميزات وفئات البيانات أمرًا شائعًا ، خاصة مع مشاريعAgile.**
- **نمذجة التهديد ، والتي هي في الأساس تحديد ، تعداد ، ترتيب الأولويات ، ومعالجة أولية للتهديدات ، هي أداة أساسية يجب تنفيذها كتطوير معماري وتقدم في التصميم .يمكن تحسين هندسة الأمان ، وهو عامل نموذج التهديد ، (لكل من جوانب البرامج والأجهزة) بعد مرحلة نمذجة التهديد .يتم وضع قواعد التشفير الآمن وإنشاء قائمة بأدوات الأمان التي سيتم استخدامها .تم توضيح استراتيجية اختبار الأمان .**
- **يجب تخزين جميع متطلبات الأمان واعتبارات التصميم في نظام إدارة دورة حياة التطبيق (ALM) (المعروف أيضًا باسم تعقب المشكلة) الذي يستخدمه فريق التطوير / العمليات لضمان التكامل الدقيق لمتطلبات الأمان في سير عمل التطوير .يجب أن تحتوي متطلبات الأمان على مقتطفات التعليمات البرمجية المصدر ذات الصلة حتى يتمكن المطورون من الرجوع إلى المقتطفات بسرعة .يعد إنشاء مستودع مخصص يخضع للتحكم في الإصدار ويحتوي فقط على مقتطفات التعليمات البرمجية هذه استراتيجية تشفير آمنة أكثر فائدة من الطريقة التقليدية) تخزين الإرشادات في مستندات Word أو ملفات.(PDF**
- **تطوير البرنامج بأمان .لزيادة رمز الحماية، يجب عليك إتمام الأنشطة مثل قانون الضمان التعليقات ، ساكنة تطبيق اختبار الأمن ، و حدة الأمن الاختبار .على**

II7MAD99@GMAIL.COM 26 Oct 2021

الرغم من وجود نظائر الجودة لأنشطة الأمان هذه ، يجب تطبيق نفس المنطق على الأمان ، على سبيل المثال ، مراجعة وتحليل واختبار التعليمات البرمجية للعيوب الأمنية (على سبيل المثال ، التحقق من صحة الإدخال المفقود ، والفشل في تحرير جميع الموارد ، وما إلى ذلك).

- يأتي بعد ذلك الاختبار المرشح للإصدار الذي طال انتظاره :اختبار الاختراق اليدوي والآلي .("Pentests")عادةً ما يتم إجراء اختبار أمان التطبيق الديناميكي خلال هذه المرحلة أيضًا.
- بعد البرنامج كانت معتمدة خلال القبول من قبل جميع أصحاب المصلحة، ويمكن انتقلت بسلام إلى عملية الفرق وضعت في الإنتاج.
- المرحلة الأخيرة ، التي غالبًا ما يتم تجاهلها ، هي إيقاف تشغيل البرنامج بأمان بعد انتهاء استخدامه.

توضح الصورة أدناه جميع المراحل والتحف:



١

استنادًا إلى ملف تعريف المخاطر العامة للمشروع ، يمكنك تبسيط (أو حتى تخطي) بعض القطع الأثرية ، ويمكنك إضافة أخرى (موافقات وسيطة رسمية ، وتوثيق رسمي لنقاط معينة ، وما إلى ذلك) .تذكر دائمًا شيئين: تهدف SDLC إلى تقليل المخاطر المرتبطة بتطوير البرامج ، وهي عبارة عن إطار عمل يساعدك في إعداد عناصر تحكم لتحقيق هذه الغاية .هذا وصف عام لـ SDLC ؛ قم دائمًا بتخصيص إطار العمل هذا لمشاريعك.

تحديد استراتيجية الاختبار

تحدد استراتيجيات الاختبار الاختبارات التي سيتم إجراؤها أثناء SDLC وكذلك اختبار التردد .تُستخدم استراتيجيات الاختبار للتأكد من أن منتج البرنامج النهائي يلبي أهداف الأمان ، والتي يتم تحديدها بشكل عام بواسطة فرق العمل القانونية / التسويقية /

II7MAD99@GMAIL.COM 26 Oct 2021

الشركات .عادةً ما يتم إنشاء استراتيجية الاختبار أثناء مرحلة التصميم الآمن ، بعد توضيح المخاطر (أثناء مرحلة البدء) وقبل بدء تطوير الكود (مرحلة التنفيذ الآمن) .تتطلب الاستراتيجية مدخلات من أنشطة مثل إدارة المخاطر ونمذجة التهديدات السابقة وهندسة الأمن.

لا يلزم كتابة استراتيجية الاختبار رسميًا: يمكن وصفها من خلال القصص (في المشاريع الرشيقة) ، أو تعدادها سريعًا في قوائم المراجعة ، أو تحديدها كحالات اختبار لأداة معينة .ومع ذلك ، يجب بالتأكيد مشاركة الاستراتيجية لأنه يجب تنفيذها من قبل فريق آخر غير الفريق الذي حددها .علاوة على ذلك ، يجب أن توافق عليه جميع الفرق الفنية للتأكد من أنها لا تضع أعباء غير مقبولة على أي منهم.

تتناول استراتيجيات الاختبار موضوعات مثل ما يلي:

- الأهداف ووصف المخاطر
- خطط لتحقيق الأهداف ، والحد من المخاطر ، وما الاختبارات التي ستكون إلزامية ، ومن سيقوم بها ، وكيف ومتى سيتم إجراؤها
- معايير القبول

لتتبع تقدم استراتيجية الاختبار وفعاليتها ، يجب تحديد المقاييس وتحديثها باستمرار أثناء المشروع وإبلاغها بشكل دوري .يمكن كتابة كتاب كامل حول اختيار المقاييس ذات الصلة ؛ أكثر ما يمكننا قوله هنا هو أنها تعتمد على ملفات تعريف المخاطر والمشاريع والمؤسسات .تشمل أمثلة المقاييس ما يلي:

- عدد القصص المتعلقة بالضوابط الأمنية التي تم تنفيذها بنجاح
- تغطية الكود لاختبارات الوحدة للضوابط الأمنية والميزات الحساسة
- عدد الأخطاء الأمنية التي تم العثور عليها لكل بناء عبر أدوات التحليل الثابتة
- الاتجاهات في تراكم الأخطاء الأمنية (والتي يمكن تصنيفها حسب الحاجة الملحة)

هذه مجرد اقتراحات .قد تكون المقاييس الأخرى أكثر صلة بمشروعك .المقاييس هي أدوات قوية للسيطرة على المشروع ، بشرط أن تمنح مديري المشروع منظورًا واضحًا ومركبًا حول ما يحدث وما يحتاج إلى تحسين.

من المهم التمييز بين الاختبارات التي يقوم بها فريق داخلي والاختبارات التي يقوم بها طرف ثالث مستقل .عادةً ما تكون الاختبارات الداخلية مفيدة لتحسين العمليات اليومية ، بينما تكون الاختبارات الخارجية أكثر فائدة للمؤسسة بأكملها .يمكن إجراء الاختبارات الداخلية في كثير من الأحيان ، ولكن يتم إجراء اختبار الطرف الثالث مرة أو مرتين في السنة على الأكثر ؛ أيضا ، الأولى أقل تكلفة من الثانية .كلاهما ضروري ، والعديد من اللوائح تفرض اختبارات من طرف ثالث مستقل لأن مثل هذه الاختبارات يمكن أن تكون أكثر موثوقية.

II7MAD99@GMAIL.COM 26 Oct 2021

اختبار الأمان في الشلال

ما هو الشلال وكيف يتم ترتيب أنشطة الاختبار

بشكل أساسي ، لا يفرض SDLC استخدام أي دورة حياة تطوير: من الآمن القول أنه يمكن (ويجب) معالجة الأمن في أي موقف.

كانت منهجيات الشلال شائعة قبل القرن الحادي والعشرين .أشهر تطبيق يسمى "نموذج "V، حيث يتم تنفيذ المراحل بالتسلسل ويمكنك التراجع خطوة واحدة فقط .تحدث أنشطة الاختبار لهذا النموذج بالتسلسل ويتم إجراؤها ككل ، في الغالب عند نقطة في دورة الحياة عندما يكتمل تطوير التطبيق .يعني تسلسل النشاط هذا أنه من الصعب تغيير البنية والعوامل الأخرى التي تم إعدادها في بداية المشروع على الرغم من إمكانية تغيير الكود بعد تحديد العيوب.

اختبار الأمان لـ Agile / DevOps وDevSecOps

يشير DevOps إلى الممارسات التي تركز على التعاون الوثيق بين جميع أصحاب المصلحة المشاركين في تطوير البرامج) تسمى بشكل عام (Devs والعمليات) تسمى عمومًا .(Ops لا تتعلق DevOps بدمج Devs و .Ops عملت فرق التطوير والعمليات في الأصل في صوامع ، عندما قد يستغرق دفع البرامج المطورة إلى الإنتاج وقتًا طويلاً .عندما جعلت فرق التطوير نقل المزيد من عمليات التسليم إلى الإنتاج أمرًا ضروريًا من خلال العمل مع Agile ، كان على فرق التشغيل الإسراع لتتناسب مع الوتيرة DevOps .هو التطور الضروري لحل هذا التحدي من حيث أنه يسمح بإصدار البرامج للمستخدمين بسرعة أكبر .يتم تحقيق ذلك إلى حد كبير من خلال أتمتة البناء الشاملة ، وعملية اختبار البرامج وإصدارها ، وتغييرات البنية التحتية) بالإضافة إلى جانب التعاون في.(DevOps

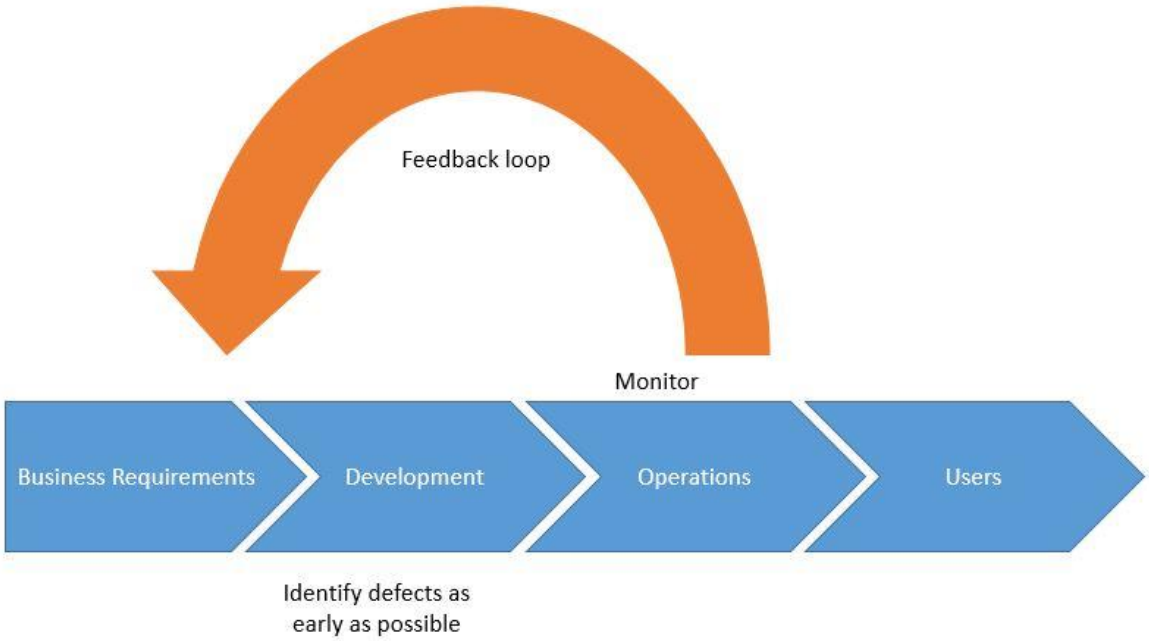
قد يفترض الناس أن مصطلح "DevOps" يمثل التعاون بين فرق التطوير والعمليات فقط ، ومع ذلك ، كما قال قائد فكر DevOps جين كيم: "للوهلة الأولى ، يبدو أن المشكلات هي فقط بين Devs و Ops ، ولكن الاختبار هو هناك ، ولديك أهداف لأمن المعلومات ، والحاجة إلى حماية الأنظمة والبيانات. هذه هي اهتمامات الإدارة العليا ، وقد أصبحت جزءًا من صورة" .DevOps

بعبارة أخرى ، يشمل تعاون DevOps فرق الجودة وفرق الأمان والعديد من الفرق الأخرى ذات الصلة بالمشروع .عندما تسمع "DevOps" اليوم ، فمن المحتمل أن تفكر في شيء مثل . DevOpsQATestInfoSec في الواقع ، تتعلق قيم DevOpsبزيادة ليس فقط السرعة ولكن أيضًا الجودة والأمان والموثوقية والاستقرار والمرونة.

II7MAD99@GMAIL.COM 26 Oct 2021

يعد الأمان أمرًا بالغ الأهمية لنجاح الأعمال تمامًا مثل الجودة الشاملة والأداء وسهولة استخدام التطبيق .مع تقصير دورات التطوير وزيادة ترددات التسليم ، يصبح التأكد من أن الجودة والأمان مدمجين منذ البداية أمرًا ضروريًا .تدور أحداث DevSecOps حول إضافة الأمان إلى عمليات .DevOps يتم تحديد معظم العيوب أثناء الإنتاج .تحدد DevOpsأفضل الممارسات لتحديد أكبر عدد ممكن من العيوب في وقت مبكر من دورة الحياة ولتقليل عدد العيوب في التطبيق الذي تم إصداره.

ومع ذلك ، فإن DevSecOps ليست مجرد عملية خطية موجهة نحو تقديم أفضل البرامج الممكنة للعمليات ؛ إنه أيضًا تفويض مفاده أن العمليات تراقب عن كثب البرامج قيد الإنتاج لتحديد المشكلات وحلها من خلال تشكيل حلقة ملاحظات سريعة وفعالة مع التطوير DevSecOps .هي عملية يتم من خلالها التأكيد بشدة على التحسين المستمر.



ينعكس الجانب الإنساني لهذا التركيز في إنشاء فرق متعددة الوظائف تعمل معًا لتحقيق نتائج الأعمال .يركز هذا القسم على التفاعلات الضرورية ودمج الأمن في دورة حياة التطوير (التي تبدأ مع بداية المشروع وتنتهي بإيصال القيمة للمستخدمين).

ما هي Agile و DevSecOps وكيف يتم ترتيب أنشطة الاختبار

ملخص

الأتمتة هي إحدى ممارسات DevSecOps الرئيسية: كما ذكرنا سابقًا ، يزداد تكرار التسليم من التطوير إلى التشغيل عند مقارنته بالنهج التقليدي ، والأنشطة التي تتطلب

II7MAD99@GMAIL.COM 26 Oct 2021

عادةً وقتًا لمواكبة ذلك ، على سبيل المثال تقديم نفس القيمة المضافة مع أخذ المزيد من الوقت .وبالتالي يجب التخلي عن الأنشطة غير المنتجة ، ويجب ربط المهام الأساسية .تؤثر هذه التغييرات على تغييرات البنية التحتية والنشر والأمان:

- يتم تنفيذ البنية التحتية كبنية أساسية ككود
- أصبح نشر أكثر كتابتها، وترجم من خلال مفاهيم مستمر التكامل و الدفع المستمر
- يتم أتمتة الأنشطة الأمنية قدر الإمكان وتجري طوال دورة الحياة

توفر الأقسام التالية مزيدًا من التفاصيل حول هذه النقاط الثلاث.

البنية التحتية كرمز

بدلاً من توفير موارد الحوسبة يدويًا (الخوادم المادية ، والآلات الافتراضية ، وما إلى ذلك) وتعديل ملفات التكوين ، تعتمد البنية التحتية كرمز على استخدام الأدوات والأتمتة لربط عملية التزويد وجعلها أكثر موثوقية وقابلية للتكرار .غالبًا ما يتم تخزين البرامج النصية المقابلة تحت التحكم في الإصدار لتسهيل المشاركة وحل المشكلات.

تعمل البنية التحتية كممارسات التعليمات البرمجية على تسهيل التعاون بين فرق التطوير والعمليات ، مع النتائج التالية:

- يفهم المطورون البنية التحتية بشكل أفضل من وجهة نظر مألوفة ويمكنهم إعداد الموارد التي يتطلبها التطبيق قيد التشغيل.
- تدير Ops بيئة تناسب التطبيق بشكل أفضل ، وتشترك في لغة مع المطورين.

تسهل البنية التحتية ككود أيضًا إنشاء البيئات التي تتطلبها مشاريع إنشاء البرامج الكلاسيكية ، من أجل التطوير ("DEV")، والتكامل ("INT")، والاختبار "PPR") لمرحلة ما قبل الإنتاج. وعادة ما يتم إجراء بعض الاختبارات في بيئات سابقة ، وتتعلق اختبارات PPR في الغالب بعدم الانحدار والأداء ببيانات مشابهة للبيانات المستخدمة في الإنتاج (والإنتاج .("PRD")تكمن قيمة البنية التحتية كرمز في التشابه المحتمل بين البيئات (يجب أن تكون هي نفسها).

تُستخدم البنية التحتية ككود بشكل شائع للمشاريع التي تحتوي على موارد قائمة على السحابة لأن العديد من البائعين يوفرون واجهات برمجة التطبيقات التي يمكن استخدامها لتزويد العناصر (مثل الأجهزة الافتراضية ومساحات التخزين وما إلى ذلك) والعمل على التكوينات (على سبيل المثال ، تعديل أحجام الذاكرة أو عدد وحدات المعالجة المركزية التي تستخدمها الأجهزة الافتراضية .(توفر واجهات برمجة التطبيقات هذه بدائل لأداء المسؤولين لهذه الأنشطة من وحدات تحكم المراقبة.

II7MAD99@GMAIL.COM 26 Oct 2021

الأدوات الرئيسية في هذا المجال هي

Puppet و Terraform و Packer و Chef و Ansible.

تعيين

يعتمد تطور خط أنابيب النشر على نضج منظمة المشروع أو فريق التطوير .في أبسط أشكاله ، يتكون خط أنابيب النشر من مرحلة الالتزام .عادةً ما تتضمن مرحلة الالتزام تشغيل عمليات تحقق بسيطة من المترجم ومجموعة اختبار الوحدة بالإضافة إلى إنشاء أداة قابلة للنشر للتطبيق .الإصدار المُرشح هو أحدث إصدار تم التحقق منه في صندوق نظام التحكم في الإصدار .يتم تقييم العناصر المرشحة للإصدار من خلال خط أنابيب النشر للتأكد من مطابقتها للمعايير التي يجب أن تفي بها للنشر في الإنتاج.

تم تصميم مرحلة الالتزام لتقديم ملاحظات فورية للمطورين ، وبالتالي يتم تشغيلها عند كل التزام بالجذع .توجد قيود الوقت بسبب هذا التردد .عادةً ما تكتمل مرحلة الالتزام في غضون خمس دقائق ، ولا ينبغي أن تستغرق أكثر من عشر دقائق .يعد الالتزام بقيد الوقت هذا أمرًا صعبًا للغاية عندما يتعلق الأمر بالأمان لأن العديد من أدوات الأمان لا يمكن تشغيلها بسرعة كافية

(#paul ،#mcgraw)

CI / CD

تعني "التكامل المستمر / التسليم المستمر" في بعض السياقات و "التكامل المستمر / النشر المستمر" في سياقات أخرى .في الواقع ، المنطق هو:

- تستخدم إجراءات بناء التكامل المستمر (إما التي يتم تشغيلها عن طريق الالتزام أو يتم تنفيذها بانتظام) كل التعليمات البرمجية المصدر لإنشاء إصدار مرشح .يمكن بعد ذلك إجراء الاختبارات والتحقق من امتثال الإصدار لقواعد الأمان والجودة وما إلى ذلك .إذا تم تأكيد الامتثال للحالة ، يمكن أن تستمر العملية ؛ خلافًا لذلك ، يجب على فريق التطوير معالجة المشكلة (المشكلات) واقتراح التغييرات.
- يمكن أن تنتقل الإصدارات المرشحة للتسليم المستمر إلى بيئة ما قبل الإنتاج .إذا كان بالإمكان بعد ذلك التحقق من صحة الإصدار (إما يدويًا أو تلقائيًا) ، فيمكن أن يستمر النشر .إذا لم يكن الأمر كذلك ، فسيتم إخطار فريق المشروع ويجب اتخاذ الإجراء (الإجراءات) المناسبة.
- يتم نقل إصدارات النشر المستمر مباشرة من التكامل إلى الإنتاج ، على سبيل المثال ، تصبح في متناول المستخدم .ومع ذلك ، لا ينبغي أن يذهب أي تحرير إلى الإنتاج إذا تم تحديد عيوب كبيرة خلال الأنشطة السابقة.

II7MAD99@GMAIL.COM 26 Oct 2021

يمكن دمج تسليم ونشر التطبيقات ذات الحساسية المنخفضة أو المتوسطة في خطوة واحدة ، ويمكن إجراء التحقق من الصحة بعد التسليم .ومع ذلك ، يُنصح بشدة بالفصل بين هذين الإجراءين واستخدام التحقق القوي للتطبيقات الحساسة.

حماية

في هذه المرحلة ، السؤال الكبير هو: الآن بعد أن تم الانتهاء من الأنشطة الأخرى المطلوبة لتقديم التعليمات البرمجية بشكل أسرع وأكثر فاعلية ، كيف يمكن للأمان مواكبة ذلك؟ كيف يمكننا الحفاظ على مستوى مناسب من الأمن؟ لن يكون تقديم قيمة للمستخدمين في كثير من الأحيان مع انخفاض مستوى الأمان أمرًا جيدًا بالتأكيد!

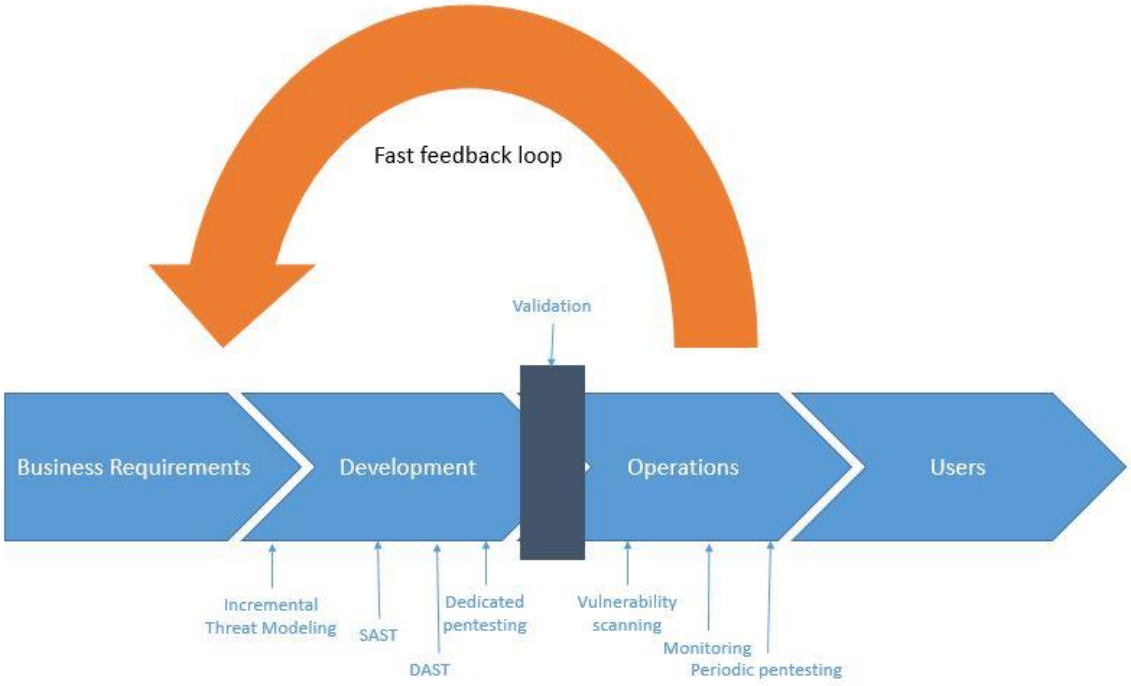
مرة أخرى ، الإجابة هي الأتمتة والأدوات: من خلال تنفيذ هذين المفهومين طوال دورة حياة المشروع ، يمكنك الحفاظ على الأمان وتحسينه .كلما ارتفع المستوى المتوقع للأمن ، زادت الضوابط ونقاط التفتيش والتركيز .فيما يلي أمثلة:

- **يمكن إجراء اختبار أمان التطبيق الثابت أثناء مرحلة التطوير ، ويمكن دمجه في عملية التكامل المستمر مع التركيز بشكل أو بآخر على نتائج الفحص .يمكنك إنشاء قواعد تشفير آمنة أكثر أو أقل طلبًا واستخدام أدوات SAST للتحقق من فعالية تنفيذها.**
- **يمكن إجراء اختبار أمان التطبيق الديناميكي تلقائيًا بعد إنشاء التطبيق (على سبيل المثال ، بعد حدوث التكامل المستمر) وقبل التسليم ، مرة أخرى ، مع تركيز أكثر أو أقل على النتائج.**
- **يمكنك إضافة نقاط التحقق اليدوية بين المراحل المتتالية ، على سبيل المثال ، بين التسليم والنشر.**

يجب مراعاة أمان التطبيق الذي تم تطويره باستخدام DevOps أثناء العمليات .فيما يلي أمثلة:

- **يجب أن يتم المسح بشكل منتظم (على مستوى كل من البنية التحتية والتطبيق).**
- **قد يتم الاعتقال بشكل منتظم) .إصدار التطبيق المستخدم في الإنتاج هو الإصدار الذي يجب أن يتم اختباره ، ويجب أن يتم الاختبار في بيئة مخصصة ويتضمن بيانات مشابهة لبيانات إصدار الإنتاج. راجع القسم الخاص باختبار الاختراق للحصول على مزيد من التفاصيل(.**
- **يجب إجراء مراقبة نشطة لتحديد المشكلات ومعالجتها في أسرع وقت ممكن عبر حلقة التغذية الراجعة.**

II7MAD99@GMAIL.COM 26 Oct 2021



مراجع

- [بول] - م. بول .الدليل الرسمي 2 (ISC) إلى CSSLP CBK ، الإصدار الثاني (ISC) 2 Press)) ، ٢٠١٤
- [مكجرو] - جي ماكجرو .أمن البرمجيات: بناء الأمن في ، ٢٠٠٦

OWASP MASVS

- " :MSTG-ARCH-1 تم تحديد جميع مكونات التطبيق ومعروف أنها مطلوبة".
- " :MSTG-ARCH-3 تم تحديد بنية عالية المستوى لتطبيق الأجهزة المحمولة وجميع الخدمات البعيدة المتصلة وتمت معالجة الأمان في تلك البنية".
- " :MSTG-ARCH-4 البيانات التي تعتبر حساسة في سياق تطبيق الهاتف المحمول محددة بوضوح".
- " :MSTG-ARCH-5 يتم تعريف جميع مكونات التطبيق من حيث وظائف العمل و / أو وظائف الأمان التي توفرها".
- " :MSTG-ARCH-6ت م إنتاج نموذج تهديد لتطبيق الجوال والخدمات البعيدة المرتبطة به والذي يحدد التهديدات المحتملة والإجراءات المضادة".
- " :MSTG-ARCH-7 جميع الضوابط الأمنية لها تنفيذ مركزي".
- " :MSTG-ARCH-10 تتم معالجة الأمان في جميع أجزاء دورة حياة تطوير البرامج.

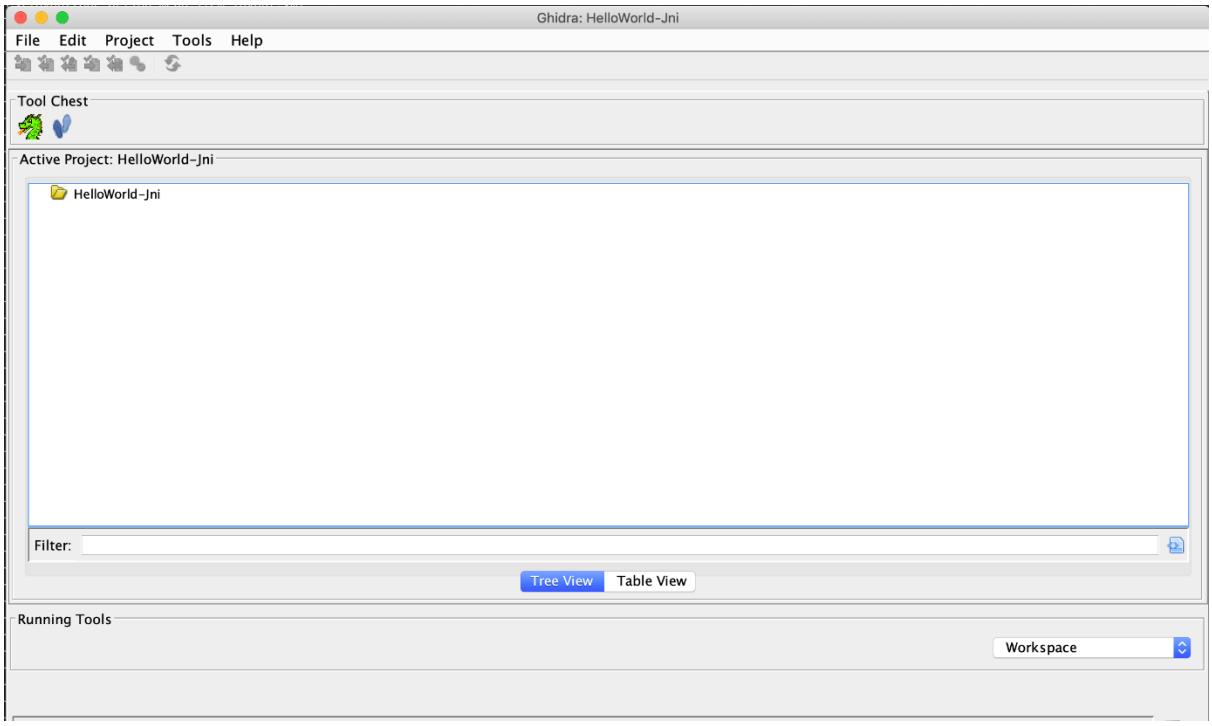
II7MAD99@GMAIL.COM 26 Oct 2021

أفضل البرامج و الأدوات

برنامج Ghidra

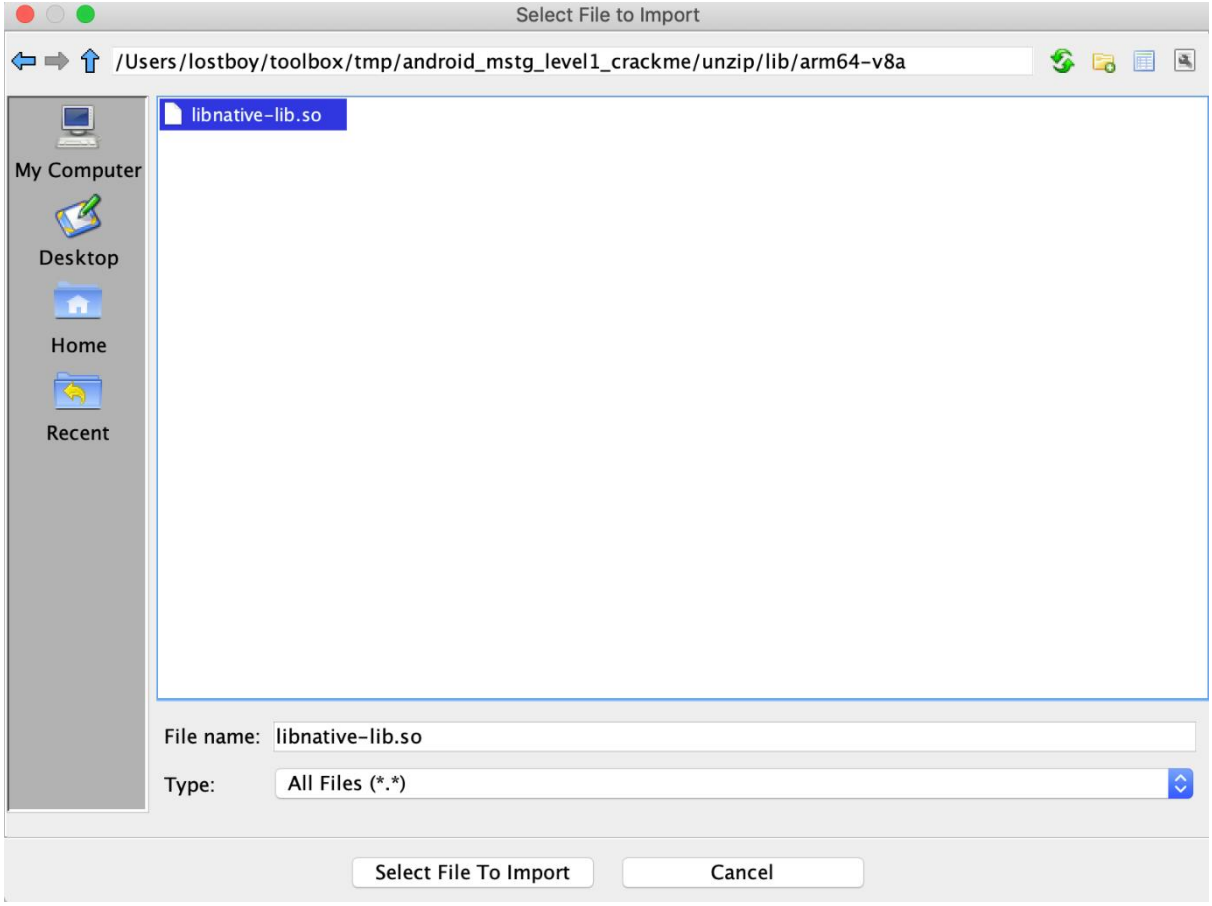
Ghidra عبارة عن مجموعة أدوات للهندسة العكسية للبرامج مفتوحة المصدر (SRE) تم تطويرها بواسطة مديرية أبحاث وكالة الأمن القومي التابعة للولايات المتحدة الأمريكية (NSA). Ghidra هي أداة متعددة الاستخدامات تتكون من مفكك ومزيل مترجم ومحرك برمجة نصية للاستخدام المتقدم .يرجى الرجوع إلى دليل التثبيت لمعرفة كيفية تثبيته وإلقاء نظرة أيضًا على ورقة الغش للحصول على نظرة عامة أولية على الأوامر والاختصارات المتاحة .في هذا القسم ، سيكون لدينا إرشادات حول كيفية إنشاء مشروع ، وعرض التفكيك والتعليمات البرمجية التي تم فك تشفيرها لثنائي.

ابدأ Ghidra باستخدام ghidraRun(* nix) أو ghidraRun.bat(Windows)، اعتمادًا على النظام الأساسي الذي تستخدمه .بمجرد تشغيل Ghidra ، قم بإنشاء مشروع جديد عن طريق تحديد دليل المشروع .سيتم الترحيب بك من خلال نافذة كما هو موضح أدناه:

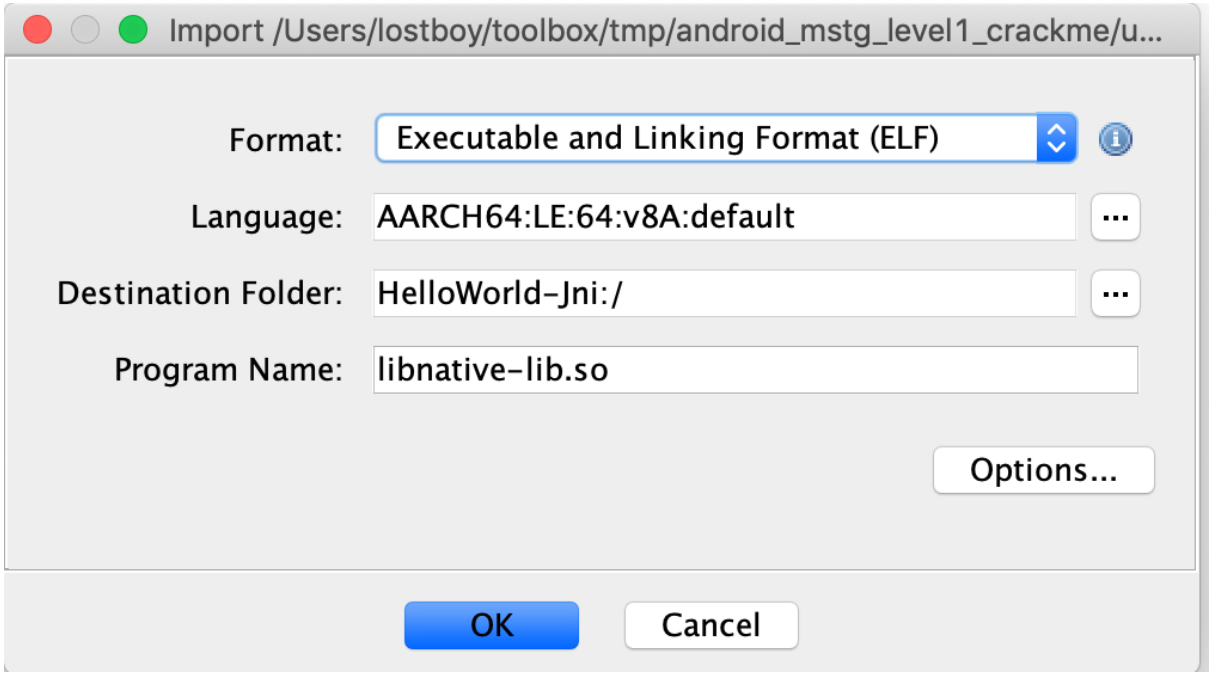


في مشروعك النشط الجديد ، يمكنك استيراد تطبيق ثنائي بالانتقال إلى ملف ثم استيراد ملف واختيار الملف المطلوب

II7MAD99@GMAIL.COM 26 Oct 2021

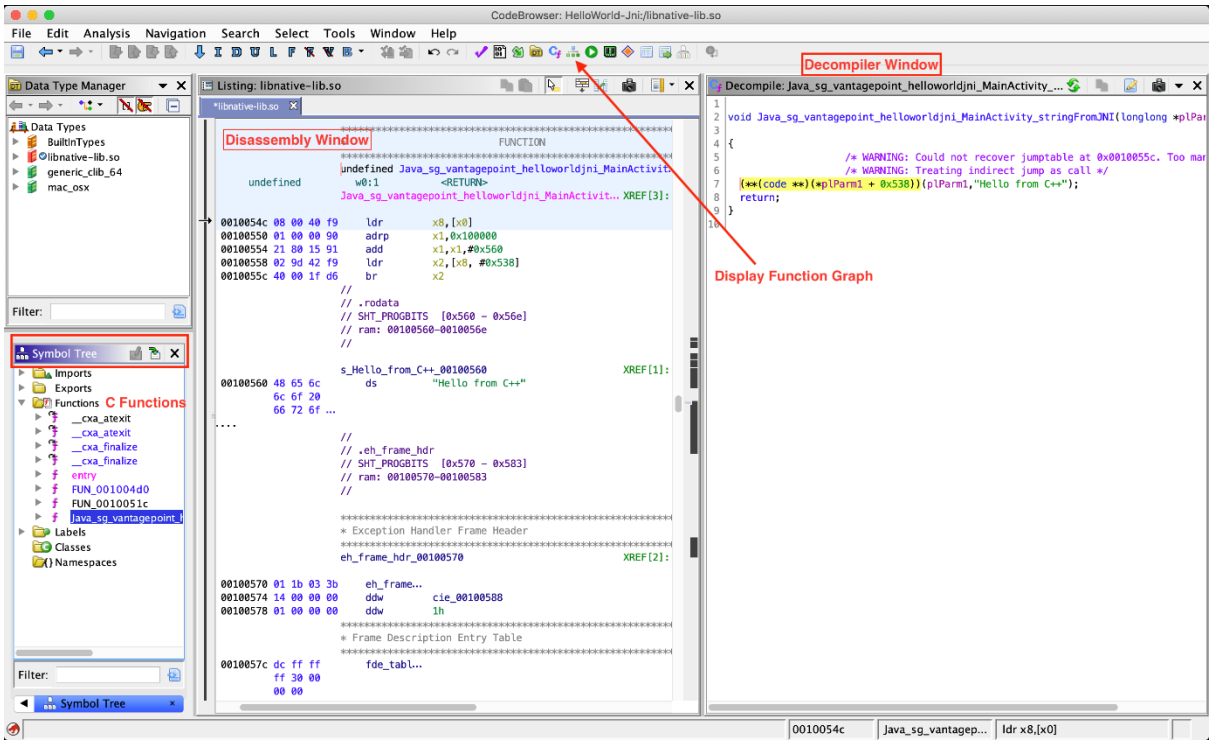


إذا كان من الممكن معالجة الملف بشكل صحيح ، فسوف يعرض Ghidra المعلومات الوصفية حول الثنائي قبل بدء التحليل



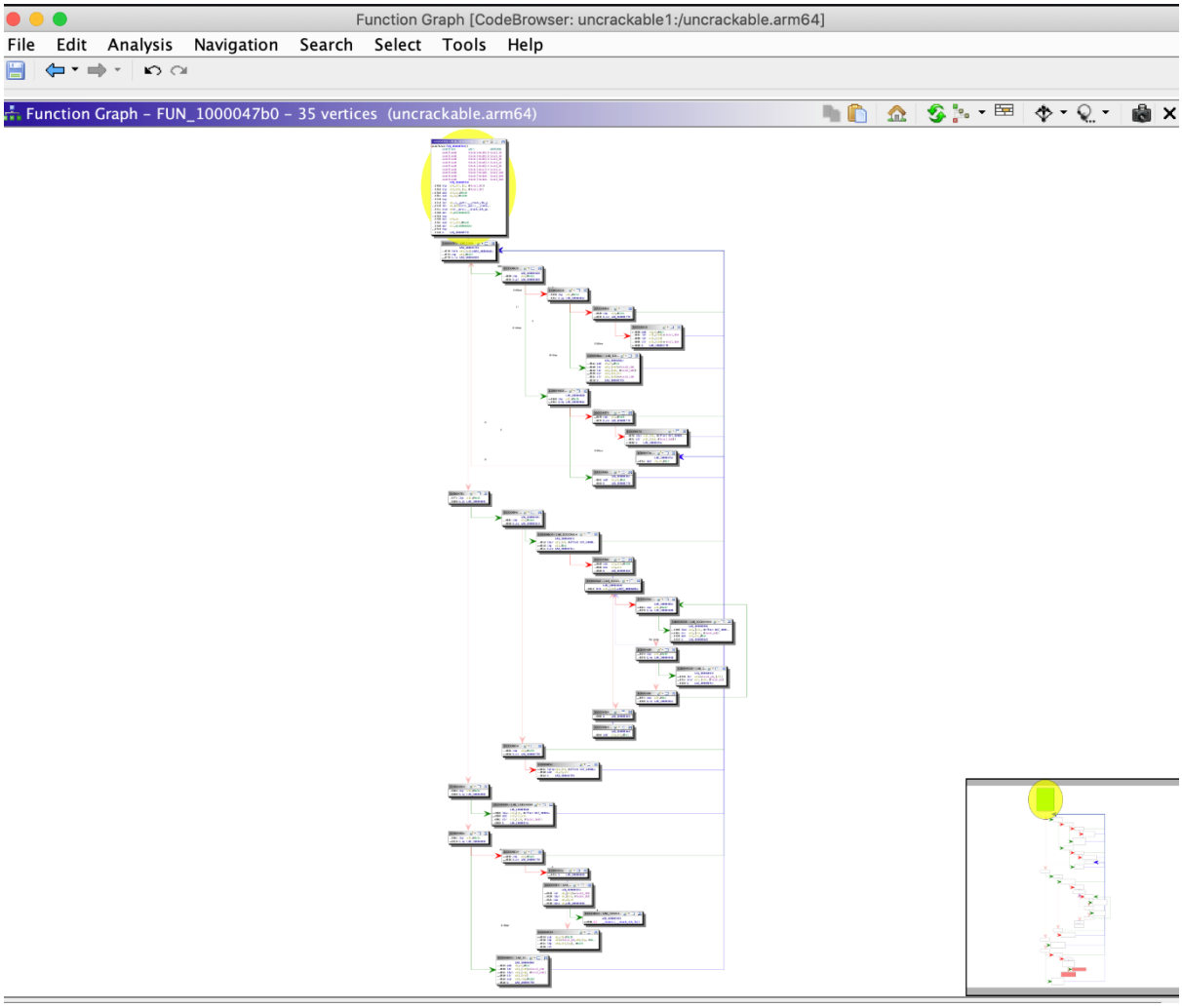
II7MAD99@GMAIL.COM 26 Oct 2021

للحصول على التعليمات البرمجية المفككة للملف الثنائي المختار أعلاه ، انقر نقرًا مزدوجًا فوق الملف المستورد من نافذة Active Project انقر فوق نعم وقم بتحليل التحليل التلقائي في النوافذ التالية سيستغرق التحليل التلقائي بعض الوقت اعتمادًا على حجم الملف الثنائي ، ويمكن تتبع التقدم في الركن الأيمن السفلي من نافذة متصفح الكود .بمجرد اكتمال التحليل التلقائي ، يمكنك البدء في استكشاف الثنائي.



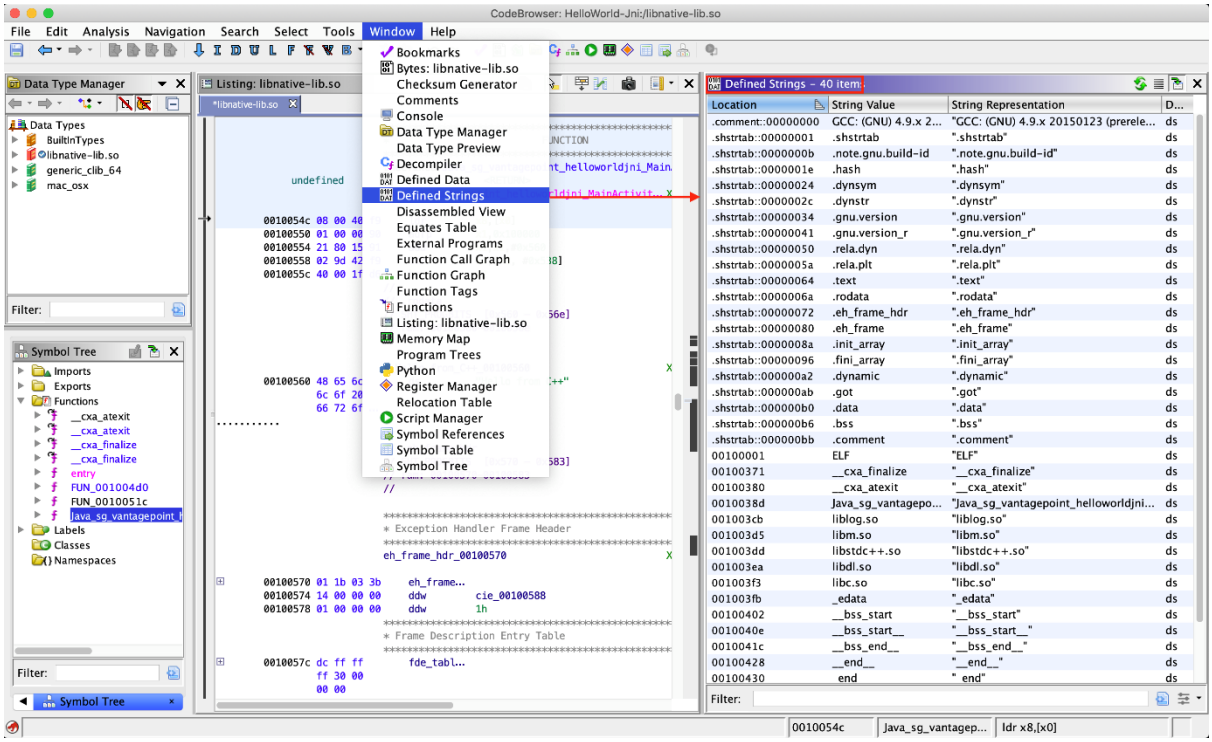
أهم النوافذ لاستكشاف ثنائي في **Ghidra** هي نافذة القائمة **(التفكيك)** ، ونافذة Symbol Tree ونافذة Decompiler ، والتي تعرض النسخة غير المجمعة من الوظيفة المحددة للتفكيك و عرض وظيفة الرسم البياني الرسم البياني التحكم في التدفق يظهر خيار الوظيفة المحددة

II7MAD99@GMAIL.COM 26 Oct 2021



هناك العديد من الوظائف الأخرى المتاحة في **Ghidra** ويمكن استكشاف معظمها من خلال فتح قائمة Window على سبيل المثال ، إذا كنت تريد فحص السلاسل الموجودة في الثنائي ، فافتح خيار Defined Strings

II7MAD99@GMAIL.COM 26 Oct 2021



برنامج Hopper

أداة هندسية عكسية لنظامي التشغيل macOS و Linux تُستخدم لتفكيك الملفات التنفيذية Intel Mac و Linux و Windows و iOS وفك تجميعها و تصحيحها

https://www.hopperapp.com

IDA Pro (أداة تجارية)

مستضاف على نظام التشغيل Windows أو Linux أو macOS برنامج تفكيك ومعالج متعدد للمعالجات

https://www.hex-rays.com/products/ida/index.shtml

برنامج LIEF

الغرض من LIEF هو توفير مكتبة عبر الأنظمة الأساسية لتحليل وتعديل وتنسيقات ELF و PE و MachO. باستخدامه ، يمكنك ، على سبيل المثال ، إدخال مكتبة معينة كتبعية لمكتبة أصلية ، والتي يقوم التطبيق بالفعل بتحميلها افتراضيًا

https://lief.quarkslab.com/

II7MAD99@GMAIL.COM 26 Oct 2021

اداة MobSF

عبارة عن إطار عمل مؤتمت متعدد الإمكانات (Mobile Security Framework) MobSF
أسهل طريقة لبدء تشغيل لتطبيقات الهاتف المحمول قادر على إجراء تحليل ثابت وديناميكي

Docker هي عبر MobSF

https://github.com/MobSF/Mobile-Security-Framework-MobSF

```
$ docker pull opensecurity/mobile-security-framework-mobsf
$ docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
```

أو قم بتثبيته وبدء تشغيله محليًا على الكمبيوتر المضيف عن طريق تشغيل:

```
# Setup
git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
cd Mobile-Security-Framework-MobSF
./setup.sh # For Linux and Mac
setup.bat # For Windows

# Installation process
./run.sh # For Linux and Mac
run.bat # For Windows
```

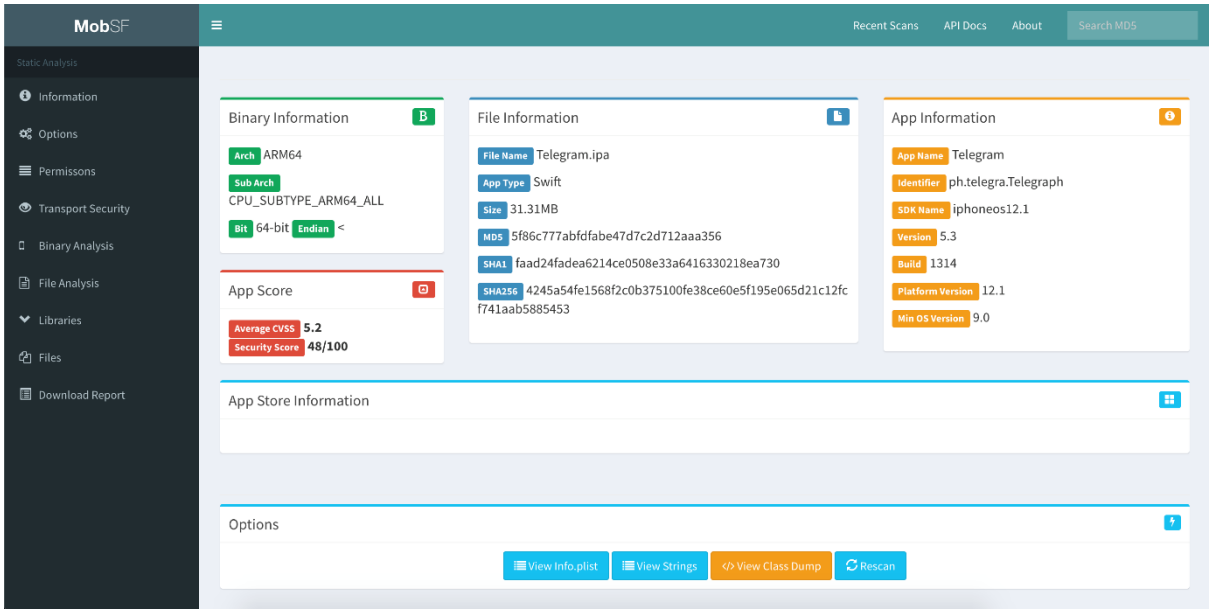
بمجرد تشغيل MobSF ، يمكنك فتحه في متصفحك بالانتقال إلى http://127.0.0.1:8000

ما عليك سوى سحب التطبيق بصيغة IPA الذي تريد تحليله إلى منطقة التحميل

وسيبدأ MobSF عمله

تتلقى نظرة عامة من صفحة واحدة لجميع الاختبارات التي تم إجراؤها .يتم تقسيم الصفحة إلى أقسام متعددة مع إعطاء بعض التلميحات الأولية على سطح الهجوم للتطبيق

II7MAD99@GMAIL.COM 26 Oct 2021



يتم عرض ما يلي:

- معلومات أساسية عن التطبيق وملفه الثنائي.
- بعض الخيارات من أجل:
  - اعرض Info.plist الملف.
  - عرض السلاسل الموجودة في التطبيق الثنائي.
  - تنزيل class-dump ، إذا كان التطبيق مكتوبًا بلغة Objective-C ؛ إذا كان مكتوبًا في Swift ، فلا يمكن إنشاء تفريغ فئة.
- قائمة بجميع سلاسل الغرض المستخرجة منها Info.plist والتي تقدم بعض التلميحات حول أذونات التطبيق
- سيتم سرد الاستثناءات في تكوين.App Transport Security (ATS)
- تحليل موجز ثنائي يوضح ما إذا تم تنشيط ميزات الأمان الثنائية المجانية أو على سبيل المثال إذا كان الثنائي يستخدم واجهات برمجة التطبيقات المحظورة
- قائمة المكتبات التي يستخدمها التطبيق الثنائي وقائمة بجميع الملفات داخل IPA الذي تم فك ضغطه

على عكس حالة استخدام Android ، لا يقدم MobSF أي ميزات تحليل ديناميكي لتطبيقات iOS
الرجوع إلى وثائق MobSF لمزيد من التفاصيل

Objection for iOS

يقدم Objection العديد من الميزات الخاصة بنظام iOS. يمكن العثور على قائمة كاملة بميزات "الاعتراض" على الصفحة الرئيسية للمشروع ، ولكن إليك بعض الميزات المثيرة للاهتمام:

II7MAD99@GMAIL.COM 26 Oct 2021

- أعد حزم التطبيقات لتشمل أداةFrida
- تعطيل تثبيت SSL للطرق الشائعة
- قم بالوصول إلى مساحة تخزين التطبيق لتنزيل الملفات أو تحميلها
- تنفيذ نصوص فريدا المخصصة
- تفريغ سلسلة المفاتيح
- اقرأ ملفاتplist

كل هذه المهام وأكثر يمكن إنجازها بسهولة باستخدام الأوامر الموجودة في REPL للاعتراض .على سبيل المثال ، يمكنك الحصول على الفئات المستخدمة في التطبيق أو وظائف الفئات أو المعلومات حول حزم التطبيق عن طريق تشغيل:

```
OWASP.iGoat-Swift on (iPhone: 12.0) [usb] # ios hooking list classes
```

```
OWASP.iGoat-Swift on (iPhone: 12.0) [usb] # ios hooking list class_methods <ClassName>
```

```
OWASP.iGoat-Swift on (iPhone: 12.0) [usb] # ios bundles list_bundles
```

تعد القدرة على إجراء تحليل ديناميكي متقدم على الأجهزة غير المعطلة إحدى الميزات التي تجعل الاعتراض مفيدًا بشكل لا يصدق .ليس من الممكن دائمًا كسر حماية أحدث إصدار من iOS ، أو قد يكون لديك تطبيق بآليات متقدمة للكشف عن كسر الحماية .علاوة على ذلك ، فإن نصوص Frida المضمنة تجعل من السهل جدًا تحليل التطبيق بسرعة ، أو الالتفاف حول ضوابط الأمان الأساسية.

أخيرًا ، في حال كان لديك حق الوصول إلى جهاز مكسور الحماية ، يمكن لـ Objects الاتصال مباشرة بخادم Frida قيد التشغيل لتوفير جميع وظائفه دون الحاجة إلى إعادة حزم التطبيق .ومع ذلك ، إذا كنت تريد الاختبار على جهاز غير مكسور الحماية ، فستحتاج أولاً إلى تضمين أداة Frida في التطبيق .و الاعتراض ويكي يصف الخطوات اللازمة في التفاصيل، ولكن بعد إجراء الاستعدادات الصحيحة، عليك أن تكون قادرا على تصحيح و IPA بالدعوة الأمر Objection :

```
$ objection patchipa --source my-app.ipa --codesign-signature 0C2E8200Dxxxx
```

أخيرًا ، يحتاج التطبيق إلى التحميل الجانبي وتشغيله مع تمكين اتصال التصحيح .يمكن العثور على خطوات مفصلة في Object Wiki، ولكن بالنسبة لمستخدمي macOS ، يمكن إجراؤها بسهولة باستخدام: ios-publish

```
$ ios-publish --bundle Payload / my-app.app -W -d
```

II7MAD99@GMAIL.COM 26 Oct 2021

باستخدام Object على iOS

يعتمد اعتراض بدء التشغيل على ما إذا كنت قد قمت بتصحيح IPA أو ما إذا كنت تستخدم جهازًا مكسور الحماية يقوم بتشغيل خادم Frida. لتشغيل IPA مصحح ، سيجد الاعتراض تلقائيًا أي أجهزة متصلة ويبحث عن أداة Frida للاستماع .ومع ذلك ، عند استخدام خادم فريدا ، فأنت بحاجة إلى إخبار خادم فريدا صراحة بالتطبيق الذي تريد تحليله

```
# الاتصال بـــ IPA

$ objection explore

# للحصول على اسم التطبيق الصحيح frida-ps استخدام اعتراض مصحح استكشاف

$ frida-ps -Ua | grep -i Telegram
983  Telegram

# توصيل إلى التطبيق من خلال التيليجرام فريدا خادم

$ objection --gadget="Telegram" explore
```

بمجرد دخولك إلى Objection REPL ، يمكنك تنفيذ أي من الأوامر المتاحة فيما يلي نظرة عامة على بعض أكثرها فائدة:

```
# Show the different storage locations belonging to the app

$ env

# Disable popular ssl pinning methods

$ ios sslpinning disable

# Dump the Keychain

$ ios keychain dump

# Dump the Keychain, including access modifiers. The result will be written to the
host in myfile.json

$ ios keychain dump --json <myfile.json>

# Show the content of a plist file

$ ios plist cat <myfile.plist>
```

II7MAD99@GMAIL.COM 26 Oct 2021

بكج أدوات

House عبارة عن مجموعة أدوات لتحليل تطبيقات الأجهزة المحمولة وقت التشغيل لتطبيقات Android، تم تطويرها وصيانتها بواسطة NCC Group وهي مكتوبة بلغة.Python

jdb

مصحح جافا يسمح بتعيين نقاط التوقف وطباعة متغيرات التطبيق .يستخدم jdb بروتوكول JDWP
- https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jdb.html

ثق بي

وحدة Xposed لتجاوز تثبيت شهادة– SSL

https://github.com/Fuzion24/JustTrustMe

بروغارد

ProGuardعبارة عن أداة تقليص ملفات فئة Java مجانية ومحسِّن ومُعتِم ومُحسِّن .يكتشف ويزيل الفئات والحقول والطرق والسمات غير المستخدمة ويمكن استخدامه أيضًا لحذف التعليمات البرمجية المتعلقة بالتسجيل.

RootCloak Plus

وحدة Cydia Substrate المستخدمة للتحقق من المؤشرات المعروفة للجذر

https://github.com/devadvance/rootcloakplus

سكربي

يوفر Scrcpy عرضًا والتحكم في أجهزة Android المتصلة عبر) USB أو). TCP / IP لا يتطلب أي وصول إلى الجذر ويعمل على GNU / Linux و macOS و Windows

SSL قيد الفتح

وحدة Xposed لتجاوز تثبيت شهادة– SSL

https://github.com/ac-pm/SSLUnpinning_Xposed

II7MAD99@GMAIL.COM 26 Oct 2021

bfinject

أداة تقوم بتحميل dylibs التعسفي لتشغيل تطبيقات App Store. يحتوي على دعم مدمج لفك تشفير تطبيقات App Store ، ويأتي مرفقًا مع iSpy و– Cycript

https://github.com/BishopFox/bfinject

برنامجBinaryCookieReader

أداة لتفريغ جميع ملفات تعريف الارتباط من ملف– binary Cookies.binarycookies

https://securitylearn.net/wp-content/uploads/tools/iOS/BinaryCookieReader.py

مساعدBurp Suite Mobile

أداة لتجاوز تثبيت الشهادة وقادرة على الحقن في التطبيقات

https://portswigger.net/burp/documentation/desktop/tools/mobile-assistant

فئة التفريغ

class-dumpبواسطة Steve Nygard هي أداة مساعدة لسطر الأوامر لفحص معلومات وقت تشغيل Objective-C المخزنة في ملفات Mach-O كائن Mach يقوم بإنشاء التصريحات للفئات والفئات والبروتوكولات

فئة تفريغ ض

تمت إعادة كتابة class-dump-z من الصفر في C ++ ، مع تجنب استخدام المكالمات الديناميكية .تؤدي إزالة هذه المكالمات غير الضرورية إلى جعل class-dump-z أسرع بنحو ١٠ مرات من سابقتها

فئة تفريغ dyld

يسمح class-dump-dyld بواسطة Elias Limneos بإلقاء الرموز واسترجاعها مباشرةً من ذاكرة التخزين المؤقت المشتركة ، مما يلغي ضرورة استخراج الملفات أولاً .يمكنه إنشاء ملفات رأس من ثنائيات التطبيق أو المكتبات أو الأطر أو الحزم أو dyld_shared_cache بالكامل .الدلائل أو كامل dyld_shared_cache يمكن تفريغها بشكل متكرر بشكل جماعي.

التشبث

يقوم Clutch بفك تشفير تطبيقات iOS وتفريغ معرف الحزمة المحدد في ملف ثنائي أو IPA - https://github.com/KJCracks/Clutch

II7MAD99@GMAIL.COM 26 Oct 2021

سايبرداك

مستعرض Libre FTP و SFTP و WebDAV و S3 و Azure و OpenStack Swift لنظامي التشغيل Mac و – Windows

https://cyberduck.io

Cycript

هي الإطار القياسي لتطوير (MobileSubstrate المعروفة سابقًا باسم Cydia Substrate) يأتي مع iOS. على (Cydia Substrate ما يسمى بامتدادات) Cydia تصحيحات وقت تشغيل C. ، وهي أداة توفر دعم حقن التعليمات البرمجية لـ Cynject

المعروف أيضًا باسم) Jay Freeman هي لغة برمجة تم تطويرها بواسطة Cycript عبر وحدة التحكم .في عملية قيد التشغيل JavaScriptCore VM يقوم بحقن .(Saurik ، يمكن للمستخدمين بعد ذلك معالجة العملية باستخدام صيغة مختلطة Cycript التفاعلية Objective-C من الممكن أيضًا الوصول إلى فئات .JavaScript و Objective-C ++ .وإنشاء مثيل لها داخل عملية قيد التشغيل

وفك ضغطه وتثبيته SDK ، قم أولاً بتنزيل Cycript لتثبيت على الايفون :

```
$ wget https://cydia.saurik.com/api/latest/3 -O cycript.zip && unzip cycript.zip
$ sudo cp -a Cycript.lib/*.dylib /usr/lib
$ sudo cp -a Cycript.lib/cycript-apl /usr/bin/cycript
```

لإنشاء غلاف Cycript التفاعلي ، قم بتشغيل "./cycript" أو "cycript" إذا كان Cycript في مسارك

```
$ cycript
cy #
```

من أول الأشياء التي يمكنك تجربتها الحصول على نسخة التطبيق (UIApplication) ، يمكنك استخدام بناء جملة: Objective-C

```
cy # [UIApplication sharedApplication]
cy # var a = [UIApplication sharedApplication]
```

II7MAD99@GMAIL.COM 26 Oct 2021

استخدم هذا المتغير الآن للحصول على فئة مفوض التطبيق:

```
cy# a.delegate
```

دعنا نحاول تشغيل رسالة تنبيه على SpringBoard باستخدام Cycript

```
cy# alertView = [[UIAlertView alloc] initWithTitle:@"OWASP MSTG" message:@"Mobile
Security Testing Guide"  delegate:nil cancelButtonitle:@"OK"
otherButtonTitles:nil]
#"<UIAlertView: 0x1645c550; frame = (0 0; 0 0); layer = <CALayer: 0x164df160>>"

cy# [alertView show]
cy# [alertView release]
```

ابحث عن دليل مستندات التطبيق باستخدام Cycript:

```
cy # [[NSFileManager defaultManager] URLsForDirectory: NSDocumentDirectory
inDomains: NSUserDomainMask] [0]
# "file: /// var / mobile / Containers / Data / Application / A8AE15EE-DC8B-4F1C-
91A5-1FED35212DF / Documents /"
```

II7MAD99@GMAIL.COM 26 Oct 2021

تعرف على المزيد http://www.cycript.org/manual

سيديا - Cydia

يمكن تثبيت العديد من الأدوات على جهاز مكسور الحماية باستخدام Cydia ، وهو متجر التطبيقات غير الرسمي لأجهزة iOS ويسمح لك بإدارة المستودعات .في Cydia ، يجب عليك إضافة المستودعات التالية (إذا لم يكن قد تم بالفعل افتراضيًا) بالانتقال إلى Edit -> Sources، ثم النقر فوق Add في الجزء العلوي الأيسر:

- : http://apt.thebigboss.org/repofiles/cydia/

أحد المستودعات الأكثر شيوعًا هو BigBoss ، والذي يحتوي على حزم متنوعة ، مثل حزمة BigBoss الموصى بها

- :أضف "Karen's Repo" للحصول على حزمة.AppSync

https://cydia.akemi.ai

- : https://build.frida.re قم بتثبيت Frida عن طريق إضافة المستودع إلى Cydia.
- : https://repo.chariz.io مفيد عند إدارة كسر الحماية على.iOS 11
- : https://apt.bingner.com/ مستودع آخر ، به عدد قليل من الأدوات الجيدة ، هو Elucubratus، والذي يتم تثبيته عند تثبيت Cydia على iOS 12 باستخدام Unc0ver.

في حال كنت تستخدم Sileo App Store ، يرجى أن تضع في اعتبارك أن طبقة توافق Sileo تشارك مصادرك بين Cydia و Sileo ، ومع ذلك ، فإن Cydia غير قادر على إزالة المصادر المضافة في Sileo ، ولا يمكن لـ Sileo إزالة المصادر المضافة في Cydia . ضع ذلك في الاعتبار عندما تحاول إزالة المصادر.
بعد إضافة جميع المستودعات المقترحة أعلاه ، يمكنك تثبيت الحزم المفيدة التالية من Cydia للبدء:

- adv-cmds: سطر أوامر متقدم ، والذي يتضمن أدوات مثل fingerd و fingerd و last وlsvfs و md و.ps
- قائمة التطبيقات: تتيح للمطورين الاستعلام عن قائمة التطبيقات المثبتة وتوفر جزء تفضيلات بناءً على القائمة

II7MAD99@GMAIL.COM 26 Oct 2021

- Apt: Advanced Package Tool، والتي يمكنك استخدامها لإدارة الحزم المثبتة بشكل مشابه لـ DPKG ، ولكن بطريقة أكثر ودية .يتيح لك ذلك تثبيت حزم وإلغاء تثبيتها وترقيتها ورجوعها إلى إصدار أقدم من مستودعات Cydia الخاصة بك .يأتي من Elucubratus.
- AppSync Unified: يسمح لك بمزامنة وتثبيت تطبيقات iOS غير الموقعة.
- أدوات BigBoss الموصى بها: تثبيت العديد من أدوات سطر الأوامر المفيدة لاختبار الأمان بما في ذلك أدوات Unix القياسية المفقودة من iOS ، بما في ذلك عميل wget و unrarو less و.sqlite3
- class-dump: أداة سطر أوامر لفحص معلومات وقت تشغيل Objective-C المخزنة في ملفات Mach-O وإنشاء ملفات رأس مع واجهات فئة.
- class-dump-z: أداة سطر أوامر لفحص معلومات وقت تشغيل Swift المخزنة في ملفات Mach-O وإنشاء ملفات رأس مع واجهات فئة .هذا غير متوفر عبر Cydia ، لذا يرجى الرجوع إلى خطوات التثبيت من أجل تشغيل class-dump-z على جهاز iOS الخاص بك .لاحظ أن class-dump-z لا تتم صيانته ولا يعمل جيدًا مع Swift. يوصى باستخدام dsdump بدلاً من ذلك.
- القابض: يستخدم لفك تشفير تطبيق قابل للتنفيذ.
- Cycript: هو مترجم مضمّن ومحسّن ومن Cycript-to-JavaScript وبيئة وحدة تحكم الوضع الفوري التي يمكن إدخالها في العمليات الجارية (المرتبطة بالركيزة).
- Cydia Substrate: نظام أساسي يجعل تطوير إضافات iOS لجهات خارجية أسهل من خلال التلاعب الديناميكي بالتطبيق أو التأمل.
- cURL: هو عميل http معروف جيدًا يمكنك استخدامه لتنزيل الحزم بشكل أسرع على جهازك .يمكن أن تكون هذه مساعدة كبيرة عندما تحتاج إلى تثبيت إصدارات مختلفة من خادم Frida على جهازك على سبيل المثال.
- أدوات Darwin CC: مجموعة مفيدة من الأدوات مثل nm و strip القادرة على تدقيق ملفات.Mach-o
- IPA Installer Console: أداة لتثبيت حزم تطبيقات IPA من سطر الأوامر .بعد تثبيت واثنين من الأوامر تكون متوفرة installipaو ipainstaller كلاهما نفس الشيء.
- فريدا: تطبيق يمكنك استخدامه للأجهزة الديناميكية .يرجى ملاحظة أن Frida قد غيرت تنفيذها لواجهات برمجة التطبيقات الخاصة بها بمرور الوقت ، مما يعني أن بعض البرامج النصية قد تعمل فقط مع إصدارات معينة من خادم Frida) مما يفرض عليك تحديث / الرجوع إلى الإصدار السابق أيضًا على .macOS) يوصى بتشغيل خادم Frida المثبت عبر APT أو .Cydia يمكن إجراء الترقية / الرجوع إلى إصدار أقدم بعد ذلك ، باتباع الإرشادات الخاصة بمشكلة Github هذه.
- Grep: أداة يدوية لتصفية الخطوط.
- Gzip: أداة ZIP معروفة جيدًا.
- PreferenceLoader: أداة مساعدة قائمة على الركيزة تسمح للمطورين بإضافة إدخالات إلى تطبيق الإعدادات ، على غرار حزم الإعدادات التي تستخدمها تطبيقات متجر التطبيقات.
- SOcket CAT: أداة يمكنك من خلالها الاتصال بمقابس لقراءة الرسائل وكتابتها .يمكن أن يكون هذا مفيدًا إذا كنت تريد تتبع سجل النظام على أجهزة iOS 12.

II7MAD99@GMAIL.COM 26 Oct 2021

إلى جانب Cydia ، هناك العديد من الأدوات مفتوحة المصدر الأخرى المتاحة ويجب تثبيتها ، مثل Introspy

إلى جانب Cydia ، يمكنك أيضًا إرسال ssh إلى جهاز iOS الخاص بك ويمكنك تثبيت الحزم مباشرةً عبر apt-get ، على سبيل المثال ، adv-cmds.

```
$apt-get update
$ apt-get install adv-cmds
```

iOS

- Crackmes: مجموعة من التطبيقات لاختبار مهاراتك في اختراق تطبيقات iOS

https://github.com/OWASP/owasp-mstg/tree/master/Crackmes

- Myriam: تطبيق iOS ضعيف مع تحديات أمان iOS

- https://github.com/GeoSn0w/Myriam

- DVIA: تطبيق iOS ضعيف مكتوب بلغة Objective-C والذي يوفر منصة لعشاق / محترفين أمن الأجهزة المحمولة أو الطلاب لاختبار مهاراتهم في اختبار اختراق– iOS

http://damnvulnerableiosapp.com/

- DVIA-v2: تطبيق iOS ضعيف ، مكتوب بلغة Swift مع أكثر من ١٥ نقطة ضعف

https://github.com/prateek147/DVIA-v2

- iGoat: تطبيق iOS Objective-C يعمل كأداة تعليمية لمطوري iOS (iPhone و iPad وما إلى ذلك (ومستخدمي تطبيقات الجوال .إنه مستوحى من مشروع WebGoat ، وله تدفق مفاهيمي مشابه له

https://github.com/owasp/igoat

II7MAD99@GMAIL.COM 26 Oct 2021

- iGoat-Swift: نسخة Swift من مشروع iGoat الأصلي

https://github.com/owasp/igoat-swift

- UnSAFE Bank: UnSAFE Bank هو تطبيق مصرفي افتراضي أساسي مصمم بهدف دمج مخاطر الأمن السيبراني وحالات الاختبار المختلفة مثل أن يتعلم المبتدئون والمطورون ومحللو الأمن مهاراتهم في تقييم نقاط الضعف واختبار الاختراق واختراقها وتحسينها

https://github.com/lucideus-repo/UnSAFE_Bank

كشف كسر الحماية

ملخص

تمت إضافة آليات الكشف عن كسر الحماية لعكس الدفاع الهندسي لجعل تشغيل التطبيق على جهاز مكسور الحماية أكثر صعوبة .يؤدي هذا إلى حظر بعض الأدوات والتقنيات التي يفضلها المهندسون العكسيون .مثل معظم أنواع الدفاع الأخرى ، فإن اكتشاف كسر الحماية ليس فعالًا جدًا بحد ذاته ، ولكن عمليات التحقق المتفرقة في جميع أنحاء كود مصدر التطبيق يمكن أن يحسن فعالية نظام مكافحة العبث بشكل عام .و نشرت قائمة أساليب الكشف عن الهروب من السجن نموذجية لدائرة الرقابة الداخلية من قبل. Trustwave

الشيكات القائمة على الملفات

تحقق من وجود ملفات وأدلة مرتبطة عادةً بعمليات كسر الحماية ، مثل:

/Applications/Cydia.app

/Applications/FakeCarrier.app

/Applications/Icy.app

/Applications/IntelliScreen.app

/Applications/MxTube.app

/Applications/RockApp.app

/Applications/SBSettings.app

/Applications/WinterBoard.app

/Applications/blackra1n.app

/Library/MobileSubstrate/DynamicLibraries/LiveClock.plist

/Library/MobileSubstrate/DynamicLibraries/Veency.plist

II7MAD99@GMAIL.COM 26 Oct 2021

/Library/MobileSubstrate/MobileSubstrate.dylib

/System/Library/LaunchDaemons/com.ikey.bbot.plist

/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist

/bin/bash

/bin/sh

/etc/apt

/etc/ssh/sshd_config

/private/var/lib/apt

/private/var/lib/cydia

/private/var/mobile/Library/SBSettings/Themes

/private/var/stash

/private/var/tmp/cydia.log

/var/tmp/cydia.log

/usr/bin/sshd

/usr/libexec/sftp-server

/usr/libexec/ssh-keysign

/usr/sbin/sshd

/var/cache/apt

/var/lib/apt

/var/lib/cydia

/usr/sbin/frida-server

/usr/bin/cycript

/usr/local/bin/cycript

/usr/lib/libcycript.dylib

/var/log/syslog

II7MAD99@GMAIL.COM 26 Oct 2021

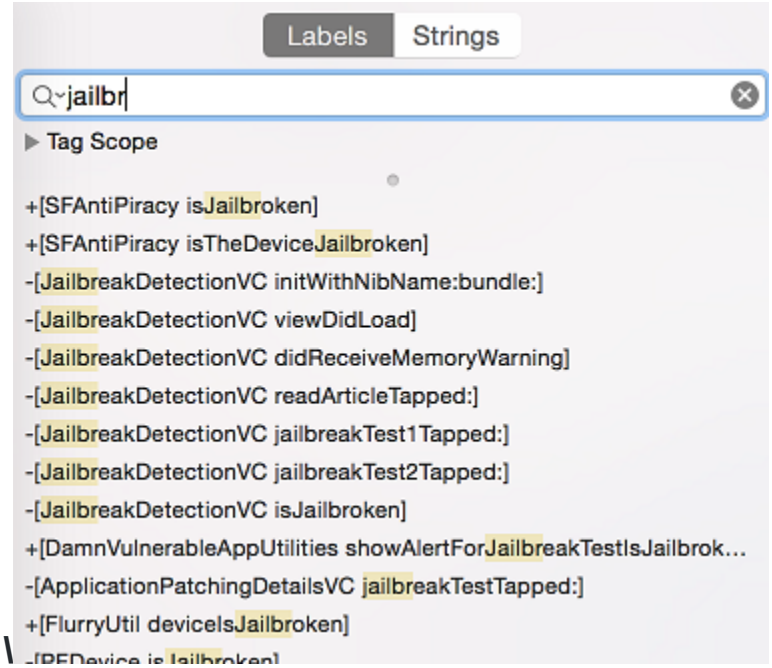
حماية كشف الجلبريك من التطبيقات

بمجرد بدء تشغيل تطبيق تم فيه تمكين اكتشاف كسر الحماية على جهاز مكسور الحماية ، ستلاحظ أحد الأشياء التالية:

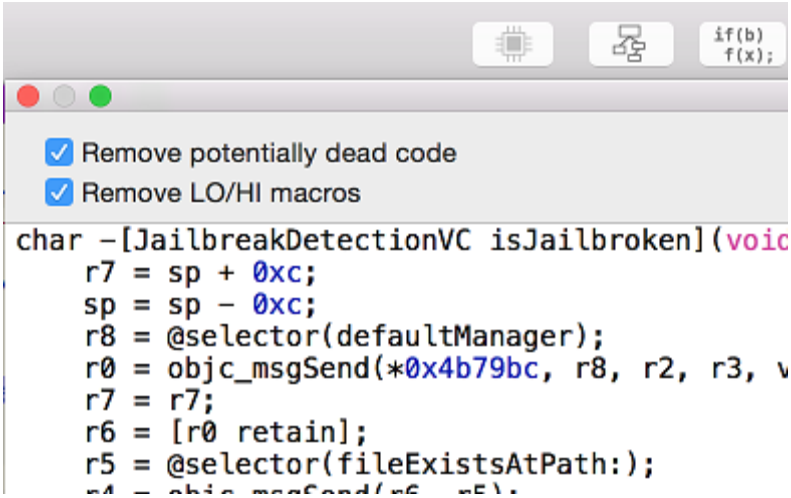
١. يتم إغلاق التطبيق على الفور دون أي إخطار.
٢. تشير النافذة المنبثقة إلى أن التطبيق لن يعمل على جهاز مكسور الحماية.

في الحالة الأولى ، تأكد من أن التطبيق يعمل بكامل طاقته على الأجهزة التي لا تحتوي على جيلبريك .قد يتعطل التطبيق أو قد يكون به خطأ يتسبب في إنهائه .قد يحدث هذا أثناء اختبار إصدار ما قبل الإنتاج من التطبيق.

لنلق نظرة على تجاوز اكتشاف كسر الحماية باستخدام تطبيق Damn Vulnerable iOS كمثال مرة أخرى .بعد تحميل الملف الثنائي في هوبر ، عليك الانتظار حتى يتم تفكيك التطبيق بالكامل (انظر إلى الشريط العلوي للتحقق من الحالة) .ثم ابحث عن سلسلة "jail" في مربع البحث .سترى فصلين SFAntiPiracy: و JailbreakDetectionVC. قد ترغب في فك الدالات لترى ما تفعله ، وعلى وجه الخصوص ، ما الذي ستعود إليه



II7MAD99@GMAIL.COM 26 Oct 2021



كما ترى ، هناك طريقة فئة **+[SFAntiPiracy isTheDeviceJailbroken]** وطريقة **-[JailbreakDetectionVC isJailbroken].** يتمثل الاختلاف الرئيسي في أنه يمكننا حقن **Cycript** في التطبيق واستدعاء طريقة **class** مباشرة ، بينما تتطلب طريقة المثيل البحث أولاً عن مثيلات الفئة المستهدفة**choose**. ستبحث الوظيفة في كومة الذاكرة عن التواقيع المعروفة لفئة معينة وتعيد مجموعة من الأمثلة. من المهم وضع تطبيق في الحالة المرغوبة (بحيث يتم إنشاء مثيل للفئة بالفعل).

دعنا نحقن **Cycript** في عمليتنا ابحث عن **PID** الخاص بك باستخدام **top:**

```
iOS8-jailbreak:~ root# cycript -p 12345
cy# [SFAntiPiracy isTheDeviceJailbroken]
true
```

كما ترى ، تم استدعاء طريقة الفصل الخاصة بنا مباشرة ، وعادت "صواب". الآن ، دعنا نسمي

- **[JailbreakDetectionVC isJailbroken]** طريقة المثيل. أولاً ، علينا استدعاء **choose** الوظيفة للبحث عن حالات **JailbreakDetectionVC** الفئة

```
cy# a=choose(JailbreakDetectionVC)
[]
```

القيمة المعادة هي صفيف فارغ. هذا يعني أنه لا توجد مثيلات لهذه الفئة مسجلة في وقت التشغيل. في الواقع ، لم ننقر على زر "اختبار جيلبريك" الثاني ، والذي يقوم بتهيئة هذه الفئة:

```
cy# a=choose(JailbreakDetectionVC)
[#"<JailbreakDetectionVC: 0x14ee15620>"]
cy# [a[0] isJailbroken]
True
```

II7MAD99@GMAIL.COM 26 Oct 2021

أنت الآن تفهم سبب أهمية وجود طلبك في الحالة المرغوبة .في هذه المرحلة ، يعد تجاوز اكتشاف كسر الحماية باستخدام Cycript أمرًا تافهًا .يمكننا أن نرى أن الدالة ترجع قيمة منطقية ؛ نحن فقط بحاجة إلى استبدال القيمة المعادة .يمكننا استبدال قيمة الإرجاع عن طريق استبدال تنفيذ الوظيفة بـ Cycript. يرجى ملاحظة أن هذا سيحل بالفعل محل الوظيفة الموجودة تحت اسمها المحدد ، لذا احذر من الآثار الجانبية إذا كانت الوظيفة تعدل أي شيء في التطبيق:

```
cy# JailbreakDetectionVC.prototype.isJailbroken=function(){return false}
cy# [a[0] isJailbroken]
false
```

II7MAD99@GMAIL.COM 26 Oct 2021

في هذه الحالة ، تجاوزنا الكشف عن كسر الحماية للتطبيق!

الآن ، تخيل أن التطبيق يغلق على الفور بعد اكتشاف أن الجهاز مكسور الحماية .ليس لديك الوقت لبدء تشغيل Cycript واستبدال تنفيذ الوظيفة .بدلاً من ذلك ، يجب عليك استخدام CydiaSubstrate، واستخدام وظيفة ربط مناسبة مثل MSHookMessageEx، وتجميع القرص .هناك مصادر جيدة لكيفية القيام بذلك ؛ ومع ذلك ، باستخدام Frida ، يمكننا بسهولة أداء الأجهزة المبكرة ويمكننا البناء على مهاراتنا المجمعة من الاختبارات السابقة

II7MAD99@GMAIL.COM 26 Oct 2021

مقدمـــة ٤
نبذه عن التطبيقات ٧
تثبيت الأساسيات Burp suite.....٢٩
فحص تطبيق soundCloud..... ٣٠
فحص تطبيق twitter..... ٣٦
فحص تطبيق tiktok..... ٥٢
فحص تطبيق snapchat.....٥٩
فحص تطبيق instagram.....٧٠
تفكيك التطبيقات..... ٨٢
فحص Netflix..... ٨٧
تثبيت الأساسيات Charles
تثبيت الأساسيات mitmproxy
اسرار التطبيقات ٩٧
أ- ماهي عادة ليست اسرار على تطبيقات الايفون
ب- لماذا تعتبر تضمين الاسرار في التطبيقات الجوال فكرة سيئة
التحليل الديناميكي.....١٠٠
التحليل الساكن ١٠٢
اهم ٤ عيوب امنيه في التطبيقات الهاتف.....١٠٦
فحص تطبيقات الايفون من الايفون.....١٠٧ - ١١٥
تحليل التطبيقات الطب الشرعي.....١١٦
التحقق من برامج التجسس.....١١٩
السجلات المستخرجه.....١٢١
تفريغ ملفات النظام
استرجاع البيانات.....١٢٥
جمع معلومات التطبيق.....١٢٧
مفتاح نظام الملفات وتغليفها.....١٣٦
ثبات البيانات ١٤٠
التحليل الديناميكي xcoed.....١٤٢

II7MAD99@GMAIL.COM 26 Oct 2021

البحث عن ملفات الارتباط.....١٤٣
البحث عن القواعد ١٤٤
مراجعه التعليمات البرمجية اليدويه.....١٤٦
التحليل الديناميكي ١٥٧
المبادئ التوجيهية ١٦٤
اختبار امان الشلال.....١٦٩
البنيه التحتيه كرمز ١٧١
الأدوات الرئيسية في المجال.....١٧٢
افضل البرامج و الادوات.....١٧٥
كشف كسر الحماية.....١٩١
الخاتمه.....١٩٩-٢٠٠

أشخاص و أماكن يجب معرفتها

II7MAD99@GMAIL.COM 26 Oct 2021

إذا كنت بحاجة إلى مساعدة باستخدام Linux Kali ، فهذه قائمة بالأشخاص و الأماكن التي يمكن انها تساعدك اكثر
تجد عبرها كل شيء ممكن أن تحتاجه

المواقع الرسمية التي ينبغي عليك زيارتها:

Homepage: http://www.kali.org
Manual and documentation: http://docs.kali.org
Blog: http://www.kali.org/blog
Source code: http://git.kali.org/gitweb

يمكن الوصول إلى community Linux Kali عبر :

Official mailing list: info@kali.org
Official forums: http://forums.kali.org
Unofficial forums: http://www.kalilinux.net
IRC: irc.freenode.net #kali-linux

يمكن متابعتي:

https://twitter.com/0xfalah
https://www.snapchat.com/add/flaah999

تم بعونه تعالى الانتهاء من هذا الكتاب عن نظام ios

لا تنسوني من صالح دعائكم
السلام عليكم ورحمة الله وبركاته

0x FaLaH